



「暗号アルゴリズム実装試験ツールの機能追加
(JCATT3の開発)」
に係る一般競争入札

入 札 関 係 書 類

- I. 入札説明書
- II. 契約書(案)
- III. 発注仕様書
- IV. 応札資料作成要領及び評価手順
- V. 評価項目一覧
- VI. その他関係資料

2011年8月22日

独立行政法人 情報処理推進機構

I. 入札説明書

独立行政法人情報処理推進機構の請負契約に係る入札公告（2011年8月22日付け公示）に基づく入札については、関係法令及び独立行政法人情報処理推進機構入札心得に定めるもののほか下記に定めるところによる。

記

1. 競争入札に付する事項

- | | |
|-----------|---|
| (1) 作業の名称 | 暗号アルゴリズム実装試験ツールの機能追加(JCATT3の開発) |
| (2) 作業内容等 | 別紙仕様書のとおり。 |
| (3) 履行期限 | 別紙仕様書のとおり。 |
| (4) 入札方法 | 落札者の決定は総合評価落札方式をもって行うので、
① 入札に参加を希望する者（以下「入札者」という。）は「6. (4) 提出書類一覧」に記載の提出書類を提出すること。
② 上記①の提出書類のうち提案書については、入札資料作成要領に従って作成、提出すること。
③ 上記①の提出書類のうち、入札書については仕様書及び契約書案に定めるところにより、入札金額を見積るものとする。入札金額は、「暗号アルゴリズム実装試験ツールの機能追加(JCATT3の開発)」に関する総価とし、総価には本件業務に係る一切の費用を含むものとする。
④ 落札決定に当たっては、入札書に記載された金額に当該金額の5パーセントに相当する額を加算した金額(当該金額に1円未満の端数が生じたときは、その端数金額を切捨てるものとする。)をもって落札価格とするので、入札者は、消費税及び地方消費税に係る課税事業者であるか免税事業者であるかを問わず、見積もった契約金額の105分の100に相当する金額を入札書に記載すること。
⑤ 入札者は、提出した入札書の引き換え、変更又は取り消しをすることはできないものとする。 |

2. 競争参加資格

- (1) 予算決算及び会計令（以下「予決令」という。）第70条の規定に該当しない者であること。
なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。
- (2) 予決令第71条の規定に該当しない者であること。
- (3) 法人税、消費税及び地方消費税について、納付期限を過ぎた未納税額がないこと。
- (4) 登記簿謄本、営業経歴書及び財務諸表を提出すること。または、平成22・23・24年度競争参加資格（全省庁統一資格）における資格を有する者であること。

3. 入札者の義務

入札者は、当機構が交付する仕様書に基づいて提案書を作成し、これを入札書に添付して入札書等の提出期限内に提出しなければならない。また、開札日の前日までの間において当機構から当該書類に関して説明を求められた場合は、これに応じなければならない。

なお、入札者の作成した提案書は当機構において審査するものとし、採用し得ると判断した提案書を添付した入札書のみを落札決定の対象とする。

4. 入札説明会の日時及び場所

- (1) 入札説明会の日時
2011年8月29日（月）14時00分
- (2) 入札説明会の場所
東京都文京区本駒込2-28-8 文京グリーンコートセンターオフィス13階
独立行政法人情報処理推進機構 会議室C
※ 入札説明会への参加を希望する場合は、15. (4)の担当部署まで電子メールにより申し込むこと。

5. 入札に関する質問の受付等

- (1) 質問の方法
質問書（様式1）に所定事項を記入の上、電子メールにより提出すること。
- (2) 受付期間
2011年8月30日（火）から2011年9月8日（木）17時00分まで。
なお、質問に対する回答に時間がかかる場合があるため、余裕をみて提出すること。
- (3) 担当部署
15. (4)のとおり

6. 入札書等の提出方法及び提出期限等

- (1) 受付期間
2011年9月13日（火）から2011年9月16日（金）まで。
持参の場合の受付時間は、月曜日から金曜日（祝祭日は除く）の10時00分から17時00分（12時30分～13時30分の間は除く）とする。
- (2) 提出期限
2011年9月16日（金）17時00分必着。
上記期限を過ぎた入札書等はいかなる理由があっても受け取らない。
- (3) 提出先
15. (4)のとおり。
- (4) 提出書類一覧

No.	提出書類	様式	部数
①	委任状（代理人に委任する場合に限る）	様式 2	1 通
②	入札書（封緘）	様式 3	1 通
③	提案書（別紙を含む）	—	4 部
④	添付資料（2 種類） 「IV. 入札資料作成要領及び評価手順」を参照のこと		4 部
⑤	補足資料（任意）		4 部
⑥	評価項目一覧	—	4 部
⑦	最新の納税証明書（その 3 の 3・「法人税」及び「消費税及地方消費税」について未納税額のない証明用）の原本又は写し	—	1 通
⑧	以下の[1]または[2]のいずれかを提出する。 [1]登記簿謄本（商業登記法第 6 条第 5 号から第 9 号までに掲げる株式会社登記簿等の謄本）、営業経歴書（会社の沿革、組織図、従業員数等の概要、営業品目、営業実績及び営業所の所在状況を含んだ書類）及び財務諸表類（直前 1 年間の事業年度分に係る貸借対照表、損益計算書及び株主資本等変動計算書）の原本又は写し	—	1 部

	[2]平成 22・23・24 年度競争参加資格（全省庁統一資格）における資格審査結果通知書の写し		
⑨	提案書受理票	様式 4	1 通

(5) 提出方法

① 入札書等提出書類を持参により提出する場合

入札書を封筒に入れ封緘し、封皮に氏名（法人の場合は商号又は名称）、宛先（15. (4) の担当者名）を記載するとともに「暗号アルゴリズム実装試験ツールの機能追加(JCATT3の開発) 一般競争入札に係る入札書在中」と朱書きし、その他提出書類一式と併せ封筒に入れ封緘し、その封皮に氏名（法人の場合はその商号又は名称）、宛先（15. (4) の担当者名）を記載し、かつ、「暗号アルゴリズム実装試験ツールの機能追加(JCATT3の開発) 一般競争入札に係る提出書類一式在中」と朱書きすること。

② 入札書等提出書類を郵便等（書留）により提出する場合

二重封筒とし、表封筒に「暗号アルゴリズム実装試験ツールの機能追加(JCATT3の開発) 一般競争入札に係る提出書類一式在中」と朱書きし、中封筒の封皮には直接提出する場合と同様とすること。

(6) 提出後

入札書等提出書類を受理した場合は、提案書受理票を入札者に交付する。なお、受理した提案書等は評価結果に関わらず返却しない。また、原則としてヒアリングを実施する。

7. 開札の日時及び場所

(1) 開札の日時

2011年9月29日（木）10時30分

(2) 開札の場所

東京都文京区本駒込2-28-8 文京グリーンコートセンターオフィス13階
独立行政法人情報処理推進機構 会議室C

8. その他の事項については、独立行政法人情報処理推進機構入札心得の定めにより実施する。

9. 入札の無効

入札公告に示した競争参加資格のない者による入札及び入札に関する条件に違反した入札は無効とする。

10. 落札者の決定方法

独立行政法人情報処理推進機構会計規程第29条の規定に基づいて作成された予定価格の制限の範囲内で、当機構が入札説明書で指定する要求事項のうち、必須とした項目の最低限の要求をすべて満たしている提案をした入札者の中から、当機構が定める総合評価の方法をもって落札者を定めるものとする。ただし、落札者となるべき者の入札価格によっては、その者により当該契約の内容に適合した履行がなされないおそれがあると認められるとき、又はその者と契約することが公正な取引の秩序を乱すこととなるおそれがある著しく不相当であると認められるときは、予定価格の範囲内の価格をもって入札をした他の者のうち、評価の最も高い者を落札者とすることがある。

11. 入札保証金及び契約保証金 全額免除

12. 契約書作成の要否 要（II. 契約書 請負契約書（案）を参照）

13. 支払の条件

契約代金は、業務の完了後、当機構が適法な支払請求書を受理した日の属する月の翌月末日までに契約金額を支払うものとする。

14. 契約者の氏名並びにその所属先の名称及び所在地

〒113-6591 東京都文京区本駒込2-28-8 文京グリーンコートセンターオフィス16階
独立行政法人情報処理推進機構 理事長 藤江 一正

15. その他

- (1) 入札者は、提出した証明書等について説明を求められた場合は、自己の責任において速やかに書面をもって説明しなければならない。なお、提出された書類をもとにヒアリングを実施する。ヒアリング時のプレゼンターは提案事業のプロジェクトマネージャであることが必要である。また、担当技術者をヒアリングに同席させること。

ヒアリングの予定日：2011年9月21日（水）

- (2) 入札結果等、契約に係る情報については、当機構のウェブサイトにて公表(注)するものとする。

- (3) 落札者は、契約締結時までに入札内訳書及び提案書の電子データを提出するものとする。

- (4) 入札説明会への参加申込み、仕様書に関する照会先、入札に関する質問の受付、入札書類の提出先

〒113-6591

東京都文京区本駒込2-28-8 文京グリーンコートセンターオフィス16階

独立行政法人情報処理推進機構 技術本部セキュリティセンター 担当：橋本、櫻井、飛田

TEL：03-5978-7545

E-mail：jcmvp-kobo@ipa.go.jp

なお、来訪する場合は、文京グリーンコートセンターオフィス13階当機構総合受付にお越しください。

- (5) 入札行為に関する照会先

独立行政法人情報処理推進機構 財務部 管理グループ 担当：千脇、逸見

TEL：03-5978-7502

E-mail：fa-bid-kt@ipa.go.jp

16. 入札説明書に係る様式一覧

(様式1)：質問書

(様式2)：委任状

(様式3)：入札書

(様式4)：提案書受理票

(注) 独立行政法人の事務・事業の見直しの基本方針(平成 22 年 12 月 7 日閣議決定)
に基づく契約に係る情報の公表について

独立行政法人が行う契約については、「独立行政法人の事務・事業の見直しの基本方針」(平成 22 年 12 月 7 日閣議決定)において、独立行政法人と一定の関係性を有する法人と契約をする場合には、当該法人への再就職の状況、当該法人との間の取引等の状況について情報を公開するなどの取組を進めるとされているところです。

これに基づき、以下のとおり、当機構との関係に係る情報を当機構のウェブサイトで公表することとしますので、所要の情報の当方への提供及び情報の公表に同意の上で、応札若しくは応募又は契約の締結を行っていただくよう御理解と御協力をお願いいたします。

なお、案件への応札若しくは応募又は契約の締結をもって同意されたものとみなさせていただきますので、ご了承ください。

(1) 公表の対象となる契約先

次のいずれにも該当する契約先

- ① 当機構において役員を経験した者(役員経験者)が再就職していること又は課長相当職以上の職を経験した者(課長相当職以上経験者)が役員、顧問等として再就職していること
 - ② 当機構との間の取引高が、総売上高又は事業収入の 3 分の 1 以上を占めていること
- ※ 予定価格が一定の金額を超えない契約や光熱水費の支出に係る契約等は対象外

(2) 公表する情報

上記に該当する契約先について、契約ごとに、物品役務等の名称及び数量、契約締結日、契約先の名称、契約金額等と併せ、次に掲げる情報を公表します。

- ① 当機構の役員経験者及び課長相当職以上経験者(当機構OB)の人数、職名及び当機構における最終職名
 - ② 当機構との間の取引高
 - ③ 総売上高又は事業収入に占める当機構との間の取引高の割合が、次の区分のいずれかに該当する旨
- 3 分の 1 以上 2 分の 1 未満、2 分の 1 以上 3 分の 2 未満又は 3 分の 2 以上
- ④ 一者応札又は一者応募である場合はその旨

(3) 当方に提供していただく情報

- ① 契約締結日時時点で在職している当機構OBに係る情報(人数、現在の職名及び当機構における最終職名等)
- ② 直近の事業年度における総売上高又は事業収入及び当機構との間の取引高

(4) 公表日

契約締結日の翌日から起算して原則として 72 日以内(4 月に締結した契約については原則として 93 日以内)

(5) 実施時期

平成 23 年 7 月 1 日以降の一般競争入札・企画競争・公募公告に係る契約及び平成 23 年 7 月 1 日以降に契約を締結した随意契約について適用します。

なお、応札若しくは応募又は契約の締結を行ったにもかかわらず情報提供等の協力をしていただけない相手方については、その名称等を公表させていただくことがあり得ますので、ご了承ください。

(様 式 1)

年 月 日

独立行政法人情報処理推進機構 技術本部セキュリティセンター 担当者殿

質 問 書

「暗号アルゴリズム実装試験ツールの機能追加(JCATT3 の開発)」に関する質問書を提出します。

法人名	
所属部署名	
担当者名	
電話番号	
E-mail	

質問書枚数
枚中
枚目

< 質問箇所について >

資料名	例) ○○書
ページ	例) P○
項目名	例) ○○概要
質問内容	

備考

1. 質問は、本様式1 枚につき1 問とし、簡潔にまとめて記載すること。
2. 質問及び回答は、IPA のホームページに公表する。(電話等による個別回答はしない。) また、質問者自身の既得情報 (特殊な技術、ノウハウ等)、個人情報に関する内容については、公表しない。

(様 式 2)

年 月 日

独立行政法人情報処理推進機構 理事長 殿

所 在 地

商号又は名称

代表者氏名
(又は代理人)

印

委 任 状

私は、下記の者を代理人と定め、「暗号アルゴリズム実装試験ツールの機能追加 (JCATT3 の開発)」の入札に関する一切の権限を委任します。

代 理 人 (又は復代理人)

所 在 地

所属・役職名

氏 名

使 用 印 鑑



(様式 3)

年 月 日

独立行政法人情報処理推進機構 理事長 殿

所在地

商号又は名称

代表者氏名

印

(又は代理人、復代理人氏名)

印

※代理人又は復代理人が入札する場合は、代表者印は特に必要としない。

入札書

入札金額 ¥ _____

入札事項 暗号アルゴリズム実装試験ツールの機能追加(JCATT3 の開発)

契約条項の内容及び貴機構入札心得を承知の上入札いたします。

(様 式 4) 提案書受理票

提案書受理票 (控)

提案書受理番号

件名:「暗号アルゴリズム実装試験ツールの機能追加(JCATT3 の開発)の入札」に関する提案書

【入札者記載欄】

提出年月日:	年	月	日
法人名:			
所在地:	〒		
担当者:	所属・役職名		
	氏名		
	TEL	FAX	
	E-Mail		

【IPA 担当者使用欄】

No.	提出書類	部数	有無	No.	提出書類	部数	有無
①	委任状 (委任する場合)	1 通		②	入札書 (封緘)	1 部	
③	提案書 (別紙を含む)	4 部					
④	添付資料 (2 種類)	4 部		⑤	補足資料 (任意)	4 部	
⑥	評価項目一覧	4 部		⑦	納税証明書	1 通	
⑧	登記簿謄本等※	1 部		⑨	提案書受理票	(本紙)	

※登記簿謄本等の原本または写し。または、資格審査結果通知書の写し。

----- 切り取り -----

提案書受理番号

「暗号アルゴリズム実装試験ツールの機能追加(JCATT3 の開発)の入札」に関する提案書 提案書受理票

年 月 日

法人名 (入札者が記載):

担当者名 (入札者が記載): 殿

貴殿から提案された表記提案書は、受理しました。

独立行政法人情報処理推進機構 技術本部セキュリティセンター

担当者名: (印)

II. 契約書（案）

20〇〇情財第〇〇号

「暗号アルゴリズム実装試験ツールの機能追加(JCATT3の開発)」に関する請負契約書（案）

独立行政法人情報処理推進機構（以下「甲」という。）と〇〇〇〇〇〇（以下「乙」という。）とは、「暗号アルゴリズム実装試験ツールの機能追加(JCATT3の開発)」について以下のとおり本契約（末尾付記の「特記事項」及び別紙1の「個人情報の取扱いに関する特則」を含む。以下同様）を締結する。

（用語の定義）

第1条 本契約において使用する用語は、情報産業分野に属する事業者間で通常理解されている意味内容を有するものとする。但し、以下の各号に掲げる用語については、当該各号が定めるところによる。

- (1)「開発成果物」とは、別添発注仕様書及び提案書（以下「仕様書等」という。）に基づいて開発されるべき別紙2記載の各物件をいう。
- (2)「本件開発業務」とは、本契約に従って開発成果物を開発する業務をいう。
- (3)「改版」とは、開発成果物の内容に加除変更を加え、または異なる記述形式で記述する（アナログ／デジタル間変換、文字／音響／画像間変換等を含む）一切の行為をいう。
- (4)「件外プロダクト」とは、開発成果物のうち、専ら本件業務のために新規に開発された部分（または要素）を除いたすべての部分（または要素）をいい、何人（甲また乙を含む。以下同様）かの制作にかかるものであるか否かを問わない。
- (5)「LPプロダクト（Legally Protected Product）」とは、件外プロダクトのうち、何人かの権利（肖像権など非財産的権利を含む）の対象となる部分（または要素）をいう。
- (6)「原プロダクト」とはLPプロダクトのうち、別紙2記載の各物件をいう。
- (7)「PDプロダクト（Public Domain Product）」とは、件外プロダクトのうち、LPプロダクトを除いたすべての部分（または要素）をいう。

（開発請負）

第2条 甲は、本件開発業務を乙に発注し、乙はこれを請負う。

2 乙は、本件開発業務の遂行にあたり、次の各号のいずれかに該当するもの（原プロダクトを除く）を開発成果物中に利用する場合、事前に様式1により利用の内容を甲に提出し、その承認を得る。

(1) 国内外の社会の健全な発展及び／または情報産業の振興に資するために開発成果物を広く普及する上で支障（法律上経済上の支障であって、その程度が軽微なものを除く）を生じ得べき件外プロダクト

(2) 第12条第1項所定の権利に基づく開発成果物の利用自体によって、対価の支払義務が生ずることとなるLPプロダクト

3 乙は、本件開発業務の全部を第三者に再請負させてはならない。

4 乙は、本件開発業務の一部を第三者に再請負させることができる。この場合甲は、再請負先の行為を全て乙の行為とみなし、乙に対し、本契約上の責任を問うことができる。

5 乙は、前項に基づき再請負させる場合、事前に再請負先、再請負の対価、再請負作業内容及び請負わせる理由等を書面により甲に届け出る。なお、再請負先からの見積書を添付するものとする。

6 乙が本件開発業務の全部または一部を第三者と共同で行う場合であっても、本契約との関係においては、第4項所定の再請負とみなす。

（交付資料の取扱）

第3条 乙は、本契約に基づいて甲から交付されたすべての資料を、本契約の目的の範囲内でのみ使用する。また、乙は、甲の同意なくこれら交付資料を複製しない。

(責任者の選任)

第4条 乙は、開発業務を実施するにあたって責任者(乙の正規従業員に限る)を選任して甲に届け出る。

2 責任者は、開発作業の進捗状況を常に把握するとともに、甲との連絡窓口として、右各進捗状況について甲の随時の照会に応じるとともに定期的または必要に応じてこれを甲に報告するものとする。

3 乙は、第1項により選任された責任者に変更がある場合は、速やかに甲に届け出る。

(納入)

第5条 乙は、別紙2の定めるところにより、開発成果物を甲に納入する。

2 乙が納入期限までに所定の納入をしない場合、甲は違約金として延滞日数1日につき第10条所定の契約金額の1000分の1に相当する額を徴収することができる。但し、天災その他乙の責に帰すことができない事由、又は甲が相当と認めた技術上の事由による場合は、この限りではない。

(件外プロダクトに関する告知)

第6条 乙は、開発成果物を納入する際、次の各号所定の事項の概要を記載した「件外プロダクトリスト」(様式2)を同時に甲に提出する。なお、該当する件外プロダクトが原プロダクトのみの場合は、第3項に従う。

(1) 件外プロダクトの一覧、及びこの内で第2条第2項所定の甲の承認の対象となったものの摘示

(2) 各件外プロダクトについて、開発成果物中に占める場所(または出現形態)、及び開発成果物中への利用の方法と態様

(3) 各LPプロダクトについて、権利者の名称と連絡先、権利の内容、開発成果物への利用に付された条件の有無・内容、並びにこの内で第2条第2項所定の甲の承認の対象となったものの摘示及び右承認の内容

(4) 各PDプロダクトについて、再入手の方法

(5) 件外プロダクトのうち、LPプロダクト及び/またはPDプロダクトへの該当の有無が不明なものについて、知れたる関係者の名称と連絡先、知れたる法的関係、及び再入手の方法

(6) 上記(1)から(5)に記載の個別事実ごとに、その秘密性の有無

2 甲は、件外プロダクトリストの記載内容について、乙に説明を求め、関連資料の閲覧及びそのコピーの提出等を求めることができる。

3 別紙2中の原プロダクトの項目に該当物件の記載がある場合、当該記載と同一内容の記載がなされた件外プロダクトリストが本条に従って提出されたものとみなす。

4 件外プロダクトリストの提出がない場合は、“該当する件外プロダクトが存在しない”旨の記載がなされた件外プロダクトリストが本条に従って提出されたものとみなす。

(権利義務の譲渡)

第7条 乙は、この契約によって生じる権利又は義務を第三者に譲渡し、又は承継させてはならない。

2 前項の規定は、本契約終了後も有効に存続する。

(実地調査)

第8条 甲は、必要があると認めるときは、乙並びに本件開発業務の再請負先に対し、自らまたはその指名する第三者をして、本件開発業務の実施状況等について、報告又は資料を求め、若しくは現場(第2条第4項の再請負先を含む)に臨んで実地に調査を行うことができる。

2 前項において、甲は乙に意見を述べ、補足資料の提出を求めることができる。

(検査、及び本件開発業務の完了)

第9条 甲は、開発成果物の納入を受けた日から30日以内に、仕様書等に基づいて検査を行い、同仕様書等に定める基準に適合しない事実を発見したときは、当該事実の概要を書面によって直ちに乙に通知する。

2 前項所定の期間内に同項所定の通知がないときは、当該期間満了日をもって開発成果物は同項所

定の検査に合格したものとみなす。

- 3 本件開発業務は、すべての開発成果物が本条による検査に合格した日をもって完了したものとみなす。この場合、甲は、完了を確認するために本件開発業務の完了通知書面を乙に交付する。
- 4 第1項及び第2項の規定は、第1項所定の通知書面に記載された指摘事実に対し、乙が適切な修正等を行い甲に再納入する場合に準用する。

(保証)

第10条 乙は、本件開発業務が完了した日から1年間、開発成果物に発見された欠陥・作動不良その他の不具合及び／または仕様書等所定の基準との不適合を、遅滞なく無償で修正する。

- 2 前項の期間経過後に発見された不具合及び不適合については、乙は、随時または甲の要請あり次第、当該不具合及び不適合に関する甲所定の情報を甲に提供する。

- 3 乙は、次の各号を保証する。

- (1) 開発成果物が第2条第2項を遵守して開発されていること。
- (2) 件外プロダクトリストの記載内容について、それが真実であり、かつ知りたる事実を秘匿していないこと。
- (3) 件外プロダクトリスト記載の法的事実関係の下で、開発成果物が何人かの著作権その他の権利を侵害していないこと。
- (4) 件外プロダクトリスト記載の法的事実関係の下で、かつ情報産業の振興及び／または国内外の社会の健全な発展に資する目的に適合する限りにおいて、第12条第1項所定の権利の円滑な行使が何人かの権利(著作権法第28条の権利、著作者人格権、著作隣接権等を含む)によって制限を受けることがないこと。

(対価の支払)

第11条 甲は、第9条第3項の規定による開発業務の完了後、乙から適法な支払請求書を受領した日の属する月の翌月末日までに、対価として、別紙2の定めるところにより所定の契約金額を乙に支払う。

(開発成果物の権利)

第12条 甲は、開発成果物の全部または一部について、これを改版しないでそのまま利用し、改版し、二次的著作物を生成し、それらを販売し、他人に販売を許諾し、その他現在及び／または将来において技術的に可能なあらゆる方法と態様によって商業的及び／または非商業的に利用するために必要かつ十分な法律上のすべての権利を、本件業務が完了した日から専有する。

- 2 前項の権利には、著作権法及び特許法所定の各権利(著作権法第27条及び第28条に定める権利を含む)のほか、将来の法改正によって創設される権利が含まれる。
- 3 乙は、第1項所定の権利に関する登録その他の手続きについて、甲に協力する。

(LPプロダクトの権利)

第13条 甲及び乙は、次の各号を確認する。

- (1) LPプロダクトの権利者は、次号の場合を除き、自己のLPプロダクトに対して有する著作権その他の権利の内容及び行使について、本契約によって何らの影響も受けない。
- (2) 乙が第10条第3項(4)所定の保証義務を履行する行為自体によって結果的に自動的かつ当然に発生している法律効果として、LPプロダクトの権利者は、第12条第1項所定の権利を正当に行行使する者に対して、自己のLPプロダクトに対して有する著作権その他の権利を原因とする法的請求を提起できない。

(責任)

第14条 第10条第3項(1)または(2)に反する事実がある場合、第11条所定の契約金額と同額を、当該事実に対する民法第420条所定の損害賠償予定額と定める。

- 2 第10条第3項(1)に反する事実がある場合、乙は、前項に基づく損害賠償に加えて、該当する件外プロダクトの削除その他の措置(これに要する費用は乙の負担とする)について甲の指示に従う。
- 3 第10条第3項(3)または(4)に反する事実がある場合、乙は、これによって甲が被る損害を第11条所定の契約金額を上限として賠償する。

- 4 前項において、件外プロダクトリスト記載の事実を甲が看過したことによる甲の損害部分については、乙は責任を免除される。

(秘密保持及び個人情報)

- 第 15 条 甲及び乙は、相互に本契約の履行過程において知り得た相手方の秘密を他に漏洩せず、また本契約の目的の範囲を超えて利用しない。但し、甲が、法令等、官公署の要求、その他公益的見地に基づいて、必要最小限の範囲で開示する場合を除く。
- 2 個人情報に関する取扱いについては、別紙 1 のとおりとする。
- 3 前各項の規定は、本契約終了後も有効に存続する。

(契約の変更)

- 第 16 条 甲又は乙は、各々、自己の責に帰すべき事由の有無を問わず、本件開発業務の実施に伴い状況が変化したり、技術上の支障が生じるなどして、仕様書等の目標を達成できず本件開発業務の全部又は一部の中止又は変更を希望する場合、本契約の変更の協議を契約の相手方に申し出ることができる。この場合、契約の相手方は、誠意をもって対応する。但し、次条による解除権の行使を妨げない。

(契約の解除等)

- 第 17 条 甲は、次の各号の一に該当する事由がある場合には、本契約を解除することができる。
- (1) 乙が本契約に違反した場合
- (2) 乙の責に帰すべき事由により、本契約を履行する見込みがないと認めるに足る客観的状況が生来した場合
- (3) 乙が、甲に対し、本件開発業務並びに本契約が定める届出及び報告に関して、不正又は虚偽の申立てをした場合
- (4) 乙が、本件開発業務と同じ内容の開発業務について、国又は公共団体等から補助等の支援を受け、または受けることとなった場合
- 2 本契約の解除が納入の後になされた場合、契約対価の支払い、権利帰属その他の法律関係は、右解除によって初めに遡って効力を失う。
- 3 第 1 項(3)から(4)に該当する事由がある場合、甲は、契約を解除せずに、乙に対して契約対価額の変更、支払済契約対価の全部若しくは一部の返還、及び／または損害の賠償を求めることができる。

(手続方法)

- 第 18 条 乙は、本契約に基づいて行う手続きについて、甲の定める様式がある場合は、これに従う。

(その他)

- 第 19 条 本契約中に法令の強行規定に違反して無効となる条項がある場合、当該条項は、当該強行規定が実質的に効力を失うまでの期間、当該強行規定の許容する範囲内であってかつ当該条項が意図する趣旨と最も近い内容に変更されたものとみなして、引き続き効力を存続する。
- 2 本契約に定めなき事項及び疑義については、甲乙双方が協議し決定する。
- 3 本契約に関する紛争については、東京地方裁判所を唯一の合意管轄裁判所とする。

特記事項

(談合等の不正行為による契約の解除)

- 第 1 条 甲は、次の各項のいずれかに該当したときは、契約を解除することができる。
- 1 本契約に関し、乙が私的独占の禁止及び公正取引の確保に関する法律（昭和 22 年法律第 54 号。以下「独占禁止法」という。）第 3 条又は第 8 条第 1 項第 1 号の規定に違反する行為を行ったことによ

り、次の各号のいずれかに該当することとなったとき

- (1) 独占禁止法第 49 条第 1 項に規定する排除措置命令が確定したとき
 - (2) 独占禁止法第 50 条第 1 項に規定する課徴金納付命令が確定したとき
 - (3) 独占禁止法第 66 条第 4 項の審決が確定したとき
 - (4) 独占禁止法第 7 条の 2 第 13 項又は第 16 項の課徴金納付命令を命じない旨の通知があったとき
- 2 本契約に関し、乙の独占禁止法第 89 条第 1 項又は第 95 条第 1 項第 1 号に規定する刑が確定したとき
- 3 本契約に関し、乙（法人の場合にあっては、その役員又は使用人を含む。）の刑法（明治 40 年法律第 45 号）第 96 条の 3 又は第 198 条に規定する刑が確定したとき

（談合等の不正行為に係る通知文書の写しの提出）

第 2 条 乙は、前条第 1 項各号のいずれかに該当することとなったときは、速やかに、次の各号の文書のいずれかの写しを甲に提出しなければならない。

- (1) 独占禁止法第 49 条第 1 項の排除措置命令書
- (2) 独占禁止法第 50 条第 1 項の課徴金納付命令書
- (3) 独占禁止法第 66 条第 4 項の審決についての審決書
- (4) 独占禁止法第 7 条の 2 第 13 項又は第 16 項の課徴金納付命令を命じない旨の通知文書

（談合等の不正行為による損害の賠償）

第 3 条 乙が、本契約に関し、第 1 条の各項のいずれかに該当したときは、甲が本契約を解除するか否かにかかわらず、かつ、甲が損害の発生及び損害額を立証することを要することなく、乙は、契約金額（本契約締結後、契約金額の変更があった場合には、変更後の契約金額）の 100 分の 10 に相当する金額（その金額に 100 円未満の端数があるときは、その端数を切り捨てた金額）を違約金（損害賠償額の予定）として甲の指定する期間内に支払わなければならない。

- 2 前項の規定は、本契約による履行が完了した後も適用するものとする。
- 3 第 1 項に規定する場合において、乙が事業者団体であり、既に解散しているときは、甲は、乙の代表者であった者又は構成員であった者に違約金の支払を請求することができる。この場合において、乙の代表者であった者及び構成員であった者は、連帯して支払わなければならない。
- 4 第 1 項の規定は、甲に生じた実際の損害額が同項に規定する損害賠償金の金額を超える場合において、甲がその超える分について乙に対し損害賠償金を請求することを妨げるものではない。
- 5 乙が、第 1 項の違約金及び前項の損害賠償金を甲が指定する期間内に支払わないときは、乙は、当該期間を経過した日から支払をする日までの日数に応じ、年 5 パーセントの割合で計算した金額の遅延利息を甲に支払わなければならない。

（暴力団関与の場合の契約の解除等）

第 4 条 甲は、乙（法人の場合にあっては、その役員又は使用人を含む。）について、暴力団員による不当な行為の防止等に関する法律（平成 3 年法律第 77 号）第 2 条に規定する暴力団又は暴力団員と関係があることが判明したときは、本契約を解除することができる。

- 2 乙が、本契約に関し、前項の規定に該当したときは、甲が本契約を解除するか否かにかかわらず、かつ、甲が損害の発生及び損害額を立証することを要することなく、乙は、契約金額（本契約締結後、契約金額の変更があった場合には、変更後の契約金額）の 100 分の 10 に相当する金額（その金額に 100 円未満の端数があるときは、その端数を切り捨てた金額）を違約金（損害賠償額の予定）として甲の指定する期間内に支払わなければならない。
- 3 前項の規定は、本契約による履行が完了した後も適用するものとする。
- 4 第 1 項に規定する場合において、乙が事業者団体であり、既に解散しているときは、甲は、乙の代表者であった者又は構成員であった者に違約金の支払を請求することができる。この場合において、乙の代表者であった者及び構成員であった者は、連帯して支払わなければならない。
- 5 第 2 項の規定は、甲に生じた実際の損害額が同項に規定する損害賠償金の金額を超える場合において、甲がその超える分について乙に対し損害賠償金を請求することを妨げるものではない。
- 6 乙が、第 2 項の違約金及び前項の損害賠償金を甲が指定する期間内に支払わないときは、乙は、当該期間を経過した日から支払をする日までの日数に応じ、年 5 パーセントの割合で計算した金額の遅延利息を甲に支払わなければならない。

本契約の締結を証するため、本契約書 2 通を作成し、双方記名押印の上、甲、乙それぞれ 1 通を保有する。

20〇〇年〇月〇日

甲 東京都文京区本駒込二丁目 28 番 8 号
独立行政法人情報処理推進機構
理事長 藤江 一正

乙 〇〇県〇〇市〇〇町〇丁目〇番〇〇号
株式会社〇〇〇〇〇〇〇〇
代表取締役 〇〇 〇〇

個人情報の取扱いに関する特則

(定 義)

第1条 本特則において、「個人情報」とは、請負業務に関する情報のうち、個人に関する情報であつて、当該情報に含まれる記述、個人別に付された番号、記号その他の符号又は画像もしくは音声により当該個人を識別することのできるもの（当該情報のみでは識別できないが、他の情報と容易に照合することができ、それにより当該個人を識別できるものを含む。）をいい、秘密であるか否かを問わない。以下各条において、右「当該個人」を「情報主体」という。

(責任者の選任)

第2条 乙は、個人情報を取扱う場合において、個人情報の責任者を選任して甲に届け出る。
2 乙は、第1項により選任された責任者に変更がある場合は、直ちに甲に届け出る。

(個人情報の収集)

第3条 乙は、請負業務遂行のため自ら個人情報を収集するときは、「個人情報の保護に関する法律」その他の法令に従い、適切且つ公正な手段により収集するものとする。

(開示・提供の禁止)

第4条 乙は、個人情報の開示・提供の防止に必要な措置を講じるとともに、甲の事前の書面による承諾なしに、第三者（情報主体を含む）に開示又は提供してはならない。但し、法令又は強制力ある官署の命令に従う場合を除く。
2 乙は、請負業務に従事する従業員以外の者に、個人情報を取り扱わせてはならない。
3 乙は、請負業務に従事する従業員のうち個人情報を取り扱う従業員に対し、その在職中及びその退職後においても個人情報を他人に開示・提供しない旨の誓約書を提出させるとともに、随時の研修・注意喚起等を実施してこれを厳正に遵守させるものとする。

(目的外使用の禁止)

第5条 乙は、個人情報を請負業務遂行以外のいかなる目的にも使用してはならない。

(複写等の制限)

第6条 乙は、甲の事前の書面による承諾を得ることなしに、個人情報を複写又は複製してはならない。但し、請負業務遂行上必要最小限の範囲で行う複写又は複製については、この限りではない。

(個人情報の管理)

第7条 乙は、個人情報を取り扱うにあたり、本特則第4条所定の防止措置に加えて、個人情報に対する不正アクセスまたは個人情報の紛失、破壊、改ざん、漏えい等のリスクに対し、合理的な安全対策を講じなければならない。
2 乙は、前項に従って講じた措置を、遅滞なく甲に書面で報告するものとする。これを変更した場合も同様とする。
3 甲は、乙に事前に通知の上乙の事業所に立入り、乙における個人情報の管理状況を調査することができる。
4 前三項に関して甲が別途に管理方法を指示するときは、乙は、これに従わなければならない。
5 乙は、請負業務に関して保管する個人情報（甲から預託を受け、或いは乙自ら収集したものを含む）について甲から開示・提供を求められ、訂正・追加・削除を求められ、或いは請負業務への利用の停止を求められた場合、直ちに且つ無償で、これに従わなければならない。

(返還等)

第8条 乙は、甲から要請があったとき、又は請負業務が終了（本契約解除の場合を含む）したときは、個人情報が含まれるすべての物件（これを複写、複製したものを含む。）を直ちに甲に返還し、又は引き渡すとともに、乙のコンピュータ等に登録された個人情報のデータを消去して復元不可能な状態とし、その旨を甲に報告しなければならない。但し、甲から別途に指示があるときは、これ

に従うものとする。

- 2 乙は、甲の指示により個人情報が含まれる物件を廃棄するときは、個人情報が発見できないよう必要な処置を施した上で廃棄しなければならない。

(記録)

第9条 乙は、個人情報の受領、管理、使用、訂正、追加、削除、開示、提供、複製、返還、消去及び廃棄についての記録を作成し、甲から要求があった場合は、当該記録を提出し、必要な報告を行うものとする。

- 2 乙は、前項の記録を請負業務の終了後5年間保存しなければならない。

(再請負)

第10条 乙が甲の承諾を得て請負業務を第三者に再請負する場合は、十分な個人情報の保護水準を満たす再請負先を選定するとともに、当該再請負先との間で個人情報保護の観点から見て本特則と同等以上の内容の契約を締結しなければならない。この場合、乙は、甲から要求を受けたときは、当該契約書面の写しを甲に提出しなければならない。

- 2 前項の場合といえども、再請負先の行為を乙の行為とみなし、乙は、本特則に基づき乙が負担する義務を免れない。

(事故)

第11条 乙において個人情報に対する不正アクセスまたは個人情報の紛失、破壊、改ざん、漏えい等の事故が発生したときは、当該事故の発生原因の如何にかかわらず、乙は、ただちにその旨を甲に報告し、甲の指示に従って、当該事故の拡大防止や収拾・解決のために直ちに応急措置を講じるものとする。なお、当該措置を講じた後ただちに当該事故及び応急措置の報告並びに事故再発防止策を書面により甲に提示しなければならない。

- 2 前項の事故が乙の本特則の違反に起因する場合において、甲が情報主体又は甲の顧客等から損害賠償請求その他の請求を受けたときは、甲は、乙に対し、その解決のために要した費用（弁護士費用を含むがこれに限定されない）を求償することができる。なお、当該求償権の行使は、甲の乙に対する損害賠償請求権の行使を妨げるものではない。
- 3 第1項の事故が乙の本特則の違反に起因する場合は、本契約第13条によって本契約が解除される場合を除き、乙は、前二項のほか、当該事故の善後策として必要な措置について、甲の別途の指示に従うものとする。

以上

1. 開発成果物（第 1 条（1））

項番	開発成果物	部数
1	取扱説明書	1 式
2	テスト報告書 障害管理表	1 式
3	設計資料	1 式
4	納入物件一覧リスト及びソースコード一覧リスト	1 式
5	ソースコード 実行用ロードモジュール（設定ファイルを含む）	1 式
6	開発成果報告書及びその概要版	1 式

詳細は、別添発注仕様書 「10.3 納入物件」を参照。

2. 原プロダクト（第 1 条（6））

なし

3. 納入（第 5 条第 1 項）

(1) 納入期限

2012 年 3 月 16 日

(2) 納入場所

東京都文京区本駒込二丁目 28 番 8 号

独立行政法人情報処理推進機構 技術本部セキュリティセンター

(3) 納入による費用負担

乙の負担

4. 対価の支払（第 11 条）

契約金額

金.〇〇, 〇〇〇, 〇〇〇円（うち消費税及び地方消費税額 金.〇, 〇〇〇, 〇〇〇円）

〇〇〇〇年〇〇月〇〇日

独立行政法人情報処理推進機構
理事長あて

株式会社〇〇〇〇〇〇〇
代表取締役 〇〇 〇〇〇

契約書第 2 条第 2 項に該当する件外プロダクトの利用承認について

〇〇〇〇年〇〇月〇〇日付け〇〇情財第〇〇〇号「件名」に関する契約書第 2 条第 2 項の規定に該当する件外プロダクトの利用について承認申請いたします。

なお、当該件外プロダクトの利用に当たっては、同契約書第 10 条第 3 項 (2) 及び (3) 並びに (4) を保証するとともに、納品時に同契約書第 6 条に基づく報告をいたします。

記

1. 利用する件外プロダクトの名称
 - ・ 〇〇〇〇〇〇〇〇〇エンジン（株式会社〇〇〇〇社製）
 - ・ 〇〇〇〇〇〇〇〇〇ツール（株式会社〇〇〇〇社製）

2. 件外プロダクト利用の内容

以上

〇〇〇〇年〇〇月〇〇日

独立行政法人情報処理推進機構
理事長あて

株式会社〇〇〇〇〇〇
代表取締役 〇〇 〇〇〇

件外プロダクトリストの提出について

〇〇〇〇年〇〇月〇〇日付け〇〇情財第〇〇〇号「件名」に関する契約書第 6 条の規定に基づき、
別添のとおり件外プロダクトリストを提出いたします。

件外プロダクトの一覧

契約番号
契約者
契約件名

通 番	件 外 プ ロ ダ ク ト の 名 称	承認対象

件外プロダクトに関する記載

番号

件外プロダクトの名称

項 目	記 載 内 容	秘 密 性 の有無
開発成果物に占める場所(または出現形態)		
開発成果物中への利用の方法と態様		
L P プロ ダ ク ト の 場 合 の 記 載 項 目	権利者の名称	
	権利者の連絡先	
	権利の内容	
	開発成果物への利用に付された条件の有無	条件有り / 条件なし
	上記条件の内容	
	第 2 条第 2 項の承認の対象か否か	
	上記承認の内容	
ク P ト D の 場 合 プロダ	PDプロダクトの再入手の方法	
場 不 合 分 明 の	知れたる関係者の名称	

*別添 1 リストに記載されたプロダクトそれぞれについて作成してください。

III. 仕様書

「暗号アルゴリズム実装試験ツールの機能追加 (JCATT3 の開発)」

開発業務内容（発注仕様書）

独立行政法人 **情報処理推進機構**

目次

1. 1.	背景	3
1. 2.	目的	3
1. 3.	用語の定義	3
2.	システムの概要	6
2. 1.	入出力ファイル及び運用方法の概略	6
2. 1. 1.	入出力ファイル	6
2. 1. 2.	JCATTの運用方法	6
2. 2.	JCATTの構成	7
2. 2. 1.	JCATTの構成	7
2. 2. 2.	JCATTの構成ファイルとデータの流れ	9
2. 2. 2. 1.	質問ファイル及び正解ファイル生成時	9
2. 2. 2. 2.	試験実行時	10
3.	開発内容	11
3. 1.	開発項目概要	11
3. 2.	開発前提条件	11
3. 3.	JCATTの動作環境	11
3. 4.	JCATTの開発環境	12
4.	開発機能詳細	13
4. 1.	Coreモジュールの開発	13
4. 1. 1.	Coreモジュール用設定ファイル	13
4. 1. 2.	GUI Coreの機能詳細	13
4. 1. 3.	CLI Coreの機能要件	18
4. 1. 4.	File I/Oモジュールの機能要件	18
4. 1. 5.	プロジェクト機能についての詳細	19
4. 2.	JCATTの完全性・不正改造検出機能	19
4. 2. 1.	署名生成機能	19
4. 2. 2.	署名検証機能	20
4. 3.	アルゴリズムプラグインの作成	20
4. 3. 1.	AES試験機能	22
4. 3. 2.	RSASSA-PSS試験機能	22
5.	参考資料	24
5. 1.	ASF01 の機能	24
5. 2.	JCATT2 の試験条件設定画面(参考)	24
5. 2. 1.	AES	24
5. 2. 2.	RSASSA-PSS	25
5. 3.	参考文献	27
6.	ドキュメント	29
6. 1.	基本設計書	29
6. 2.	詳細設計書	29
6. 3.	取扱説明書	29
7.	テスト	30
8.	事業の実施体制	30
9.	事業期間及びスケジュール	30
10.	検収関連事項	30
10. 1.	納入期限	30
10. 2.	納入場所	30
10. 3.	納入物件	31
10. 4.	検収条件	32

開発業務内容（仕様書）

1. はじめに

1.1. 背景

独立行政法人情報処理推進機構(以下「IPA」という。)では、「安心」して利用できる IT 基盤の構築・維持のため、情報セキュリティ対策の強化、整備を進めている。その一環として IPA では、暗号モジュールの適切な実装を確認するための、暗号モジュール試験及び認証制度(以下「JCMVP」という。)の正式運用を 2007 年 4 月から開始した。

JCMVP では、暗号モジュール試験に先立ち昨年度までに開発したツール(以下「JCATT」という。)を用いて暗号アルゴリズム実装試験を実施している。

1.2. 目的

JCATT のプログラム構造をモジュール化して、暗号アルゴリズムの追加を容易にすること、ファイル入出力において北米の暗号モジュール認証制度(CMVP)で使用されているツールである CAVS と同等のファイルフォーマットをサポートすること、AES 及び RSASSA-PSS のアルゴリズムプラグインを作成することを本開発の目的とする。

1.3. 用語の定義

本開発業務における用語の定義を以下に記載する。

#	用語	定義	備考
1	AES	Advanced Encryption Standard。2001 年に米国の暗号規格として規格化されたブロック暗号アルゴリズム。FIPS PUB 197 として公開されている。	
2	ASCII	American Standard Code for Information Interchange。ラテン文字や数字を中心とした 7 ビットの文字コード。	
3	ASCII 印字可能文字	ASCII に属する文字のうち、そのコードが 10 進数で 32～126 の範囲にある文字。	
4	ASF01	JCATT で使用している暗号エンジン(暗号アルゴリズムを実装したライブラリ)。経済産業省による「新世代情報セキュリティ研究開発事業(クラウドコンピューティングセキュリティ技術開発)」において、開発した暗号プリミティブのライブラリ(公募仕様書(http://www.meti.go.jp/information/data/c90710bj.html を参照)の 3.2 クラウド環境における暗号技術評価 参照)を、JCATT 用に適応させたものである。	
5	CAVP	Cryptographic Algorithm Validation Program。	http://csrc.nist.gov/groups/STM/cavp/index.html を参照。
6	CAVS	CAVP において暗号アルゴリズム実装試験に使用されているツール。	http://csrc.nist.gov/groups/STM/cavp/index.html を参照。
7	CBC	Cipher-block Chaining。ブロック暗号の利用モードの 1 つ。NIST SP800-38A で定義されている。	

8	CFB	Cipher Feedback。ブロック暗号の利用モードの1つ。NIST SP800-38A で定義されている。CFB にはパラメータ s があり、 s ビット CFB と呼ばれるが、 $s=1, 8$ の場合を特にそれぞれ CFB1、CFB8 と呼んでいる。	
9	CMVP	Cryptographic Module Validation Program。米国 NIST が運営している暗号モジュール試験及び認証制度。	http://csrc.nist.gov/groups/STM/cmvp/index.html を参照。
10	CTR	Counter。ブロック暗号の利用モードの1つ。NIST SP800-38A で定義されている。	
11	ECB	Electronic Codebook。ブロック暗号の利用モードの1つ。NIST SP800-38A で定義されている。	
12	FIPS PUB 186-3	NIST が発行している、デジタル署名に関する仕様書。	http://csrc.nist.gov/publications/fips/fips186-3/fips186-3.pdf を参照。
13	GUI	グラフィカルユーザインタフェース。	
14	IANA	Internet Assigned Numbers Authority。	
15	IDE	Integrated Development Environment。ソフトウェアの統合開発環境。	
16	ISO 8859-1	ISO/IEC 8859 の第1部で定義されたラテンアルファベットの文字コード。	
17	IUT	Implementation Under Test。試験対象の暗号実装。	
18	JCATT	Japan Cryptographic Algorithm Testing Tool。JCMVP において暗号アルゴリズム実装試験で使用するツール。	
19	JCATT2	本仕様書においては、JCATT の現行バージョン(2.2.x)を意味する。	
20	JCATT3	本仕様書においては、本開発で開発されるバージョンの JCATT を意味する。	
21	JCATT ファイルフォーマット仕様書	JCATT2 が入出力するファイルのフォーマットを規定した仕様書。 http://www.ipa.go.jp/security/jcmvp/open_documents.html から公開されている。	
22	JIS X0208	7ビット及び8ビットの2バイト情報交換用漢字集合を定義した日本工業規格。	
23	LGPL	GNU Lesser General Public Licence。Free Software Foundation が公開しているフリーソフトウェアライセンスのひとつ。	
24	MAC アドレス	Media Access Control Address。ネットワーク上の機器を特定する物理アドレス。	
25	NIST	National Institute of Standards and Technology。米国国立標準技術研究所。	
26	NIST SP800 シリーズ文書	NIST が発行している、コンピュータセキュリティに関する文書群。SP は Special Publication の略。	http://csrc.nist.gov/publications/PubsSps.html を参照。
27	NIST SP800-38A	NIST が発行している、ブロック暗号の利用モードに関する仕様書。NIST SP800 シリーズ文書の1つ。	http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf を参照
28	NIST SP800-90	NIST が発行している、疑似乱数生成アルゴリズムに関する仕様書。NIST SP800 シリーズ文書の1	http://csrc.nist.gov/publications/nistpubs

		つ。	/800-90/SP800-90revised_March2007.pdf を参照
29	OFB	Output Feedback。ブロック暗号の利用モードの 1 つ。NIST SP800-38A で定義されている。	
30	Qt	ノキアの一部門 Qt デベロップメントフレームワーク社によって開発されているクロスプラットフォームのアプリケーション・ユーザインターフェース・フレームワーク。	http://qt.nokia.com を参照。
31	RSA	Ron Rivest、Adi Shamir、Leonald Adleman によって発明された、素因数分解の困難性を利用した公開鍵暗号の方式。暗号化、復号、デジタル署名を実現することができる。	
32	RSASSA-PSS	PKCS#1 v2.1 で定義されているデジタル署名アルゴリズム。	ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf を参照
33	Shift_JIS	JIS X0208 の附属書 1 で「シフト符号化表現」として規定されている文字コード。	
34	UTF-8	ISO/IEC 10646 と Unicode で使用できる 8 ビット符号単位の文字コード。	
35	アルゴリズム	本仕様書においては、アルゴリズムは暗号アルゴリズムを意味する。	
36	暗号アルゴリズム実装試験仕様書 (ATR-01)	JCMVP における暗号アルゴリズム実装試験の試験仕様を定義した仕様書。 http://www.ipa.go.jp/security/jcmvp/open_documents.html から公開されている。「公開鍵」「共通鍵」「ハッシュ」「メッセージ認証」「乱数生成器」「鍵確立手法」の 6 編の仕様書から構成されている。	
37	ウィジェット	GUI を構成するウィンドウ、ボタン等のインタフェース部品。	
38	共有ライブラリ	単独のファイルとして実行形式のプログラムとは別に提供され、実行時に実行形式のプログラムとリンクされるライブラリ。Windows においては DLL(Dynamic Link Library)がそれに当たる。	
38	クラス	本仕様書においては、クラスとは C++言語の仕様で定めるクラスを指す。	

2. システムの概要

2.1. 入出力ファイル及び運用方法の概略

2.1.1. 入出力ファイル

JCATT は、暗号アルゴリズム実装試験の運用に際して、以下のテキストファイルを入出力する。

(1) プロジェクトファイル群

暗号アルゴリズム実装試験プロジェクトに関する情報を記録したファイル。最上位のマスターファイル、ベンダから依頼を受けた暗号アルゴリズムの実装に関する IUT 情報ファイル、暗号アルゴリズム確認の試験条件を記録する試験条件ファイルからなる。

(2) 質問ファイル(ファイルの拡張子は、req)

JCATT が生成するファイル。暗号アルゴリズムに対する入力データ及び制御情報が記録されている。暗号モジュール試験機関からベンダ側へ送る。

(3) 正解ファイル(ファイルの拡張子は、fax)

JCATT が質問ファイルと同時に生成するファイル。暗号アルゴリズムに対する入力データ、制御情報及び対応する出力データが記録されている。暗号モジュール試験機関で保存し、回答ファイルが送られてきた際に回答ファイルと比較する。

(4) 回答ファイル(ファイルの拡張子は、rsp)

ベンダ側で、質問ファイルを元に IUT が生成したテキストファイル。ベンダから暗号モジュール試験機関側へ送る。

(5) 結果ファイル(ファイルの拡張子は、out)

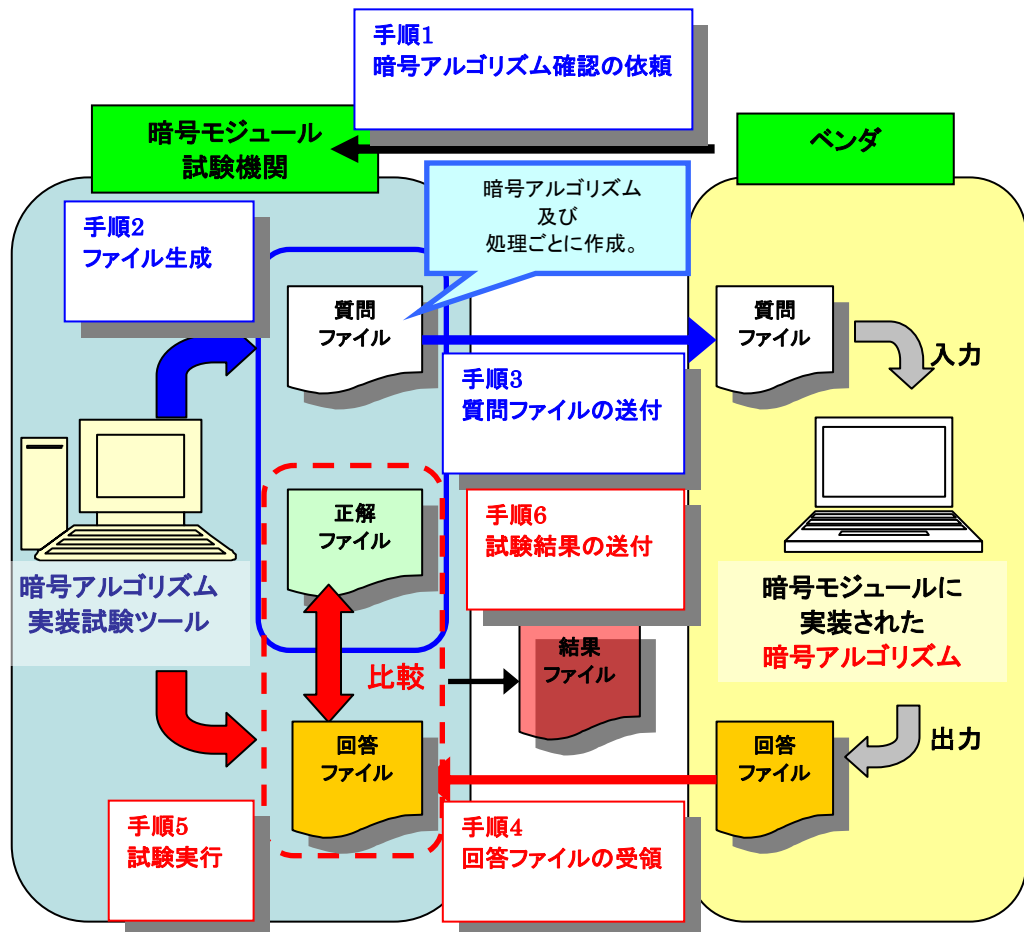
回答ファイルの内容を正解ファイルの内容と照らし合わせて、結果(正解又は不正解)を出力するファイル。

(6) エラーファイル(ファイルの拡張子は、err)

試験実施時に発生したエラーに関する情報を出力するファイル。

2.1.2. JCATTの運用方法

暗号アルゴリズム実装試験を実施する際の JCATT の運用方法の概略を下図に示す。



この運用方法を文書化すると、以下ようになる。

- 手順 1: 暗号アルゴリズム確認の依頼
暗号モジュール試験機関は、ベンダから暗号アルゴリズム確認の依頼を受け付ける。このとき、試験対象の暗号アルゴリズムと試験条件についての情報をベンダから受領する。
- 手順 2: ファイル生成
試験対象の暗号アルゴリズムを選択し、手順 1.で受領した試験条件を入力して、まずプロジェクトファイルを作成する。JCATT のファイル生成機能を使用して、プロジェクトファイルに記録された試験条件に基づく質問ファイル及び正解ファイルを作成する。
- 手順 3: 質問ファイルの送付
手順 2 で生成した質問ファイルをベンダに送付する。
- 手順 4: 回答ファイルの受領
手順 3.で送付した質問ファイルに対する回答ファイルをベンダから受領する。
- 手順 5: 試験実行
手順 4 で受領した回答ファイルと手順 2.で生成した正解ファイルを比較することにより、暗号アルゴリズム実装試験を実行する。合格及び不合格といった試験結果は、結果ファイルに記録される。
- 手順 6: 試験結果の送付
手順 5 で生成された結果ファイルをベンダに送付する。

2.2. JCATTの構成

2.2.1. JCATTの構成

JCATT3 の構成を表 1に、JCATT3 の各モジュール間の関係を図 1に示す。

構成要素		概要
Core モジュール	GUI Core	ファイル生成/試験実行/結果表示の画面を表示する GUI アプリケーション。アルゴリズムプラグインを登録し、各アルゴリズムのファイル生成機能を必要に応じて起動する。
	CLI Core	GUI Core から試験実行機能実行指示が来たときに起動される CLI プログラム。アルゴリズムプラグインを登録し、各アルゴリズムの試験実行機能を必要に応じて起動する。
	File I/O モジュール	すべてのファイル入出力に関するサービスを提供する共有ライブラリ。質問ファイル、正解ファイル書き込み時は、抽象的なリスト構造データを入力とし、具体的な書き込み内容はこのモジュール内で組み立てる。回答ファイル、正解ファイル読み込み時は、ファイルの内容を構文解析した上で上位モジュールにリスト構造データとして返す。JCATT2仕様のファイルフォーマットとJCATT3仕様(CAVS 互換)の違いの吸収も行う。設定ファイル等、暗号アルゴリズム実装試験の実施以外で使用するファイルについても、読み書きをサポートするサービスを提供する。
アルゴリズムプラグイン		1 個以上のアルゴリズムの試験機能をサポートする。試験条件入力 UI の表示、試験実行の 2 個のモジュールから成る。共有ライブラリとして作成する。組み込むプラグインは Core モジュールの設定ファイルで指定する。暗号アルゴリズム自体の実装は外部の暗号エンジンに委託する。アルゴリズムプラグインは複数組み込むことができる。
暗号エンジン(ASF01)		暗号アルゴリズムの計算(アルゴリズムに従った暗号化、復号、署名生成等の計算)が実装された共有ライブラリ。サポートされる暗号アルゴリズムには、AES(鍵長 128/192/256 ビット、暗号化/復号、ECB/CBC/CFB/CFB1/CFB8/OFB/CTR)、RSASSA-PSS(署名作成/署名検証)、NIST SP800-90 に基づく疑似乱数生成器等が含まれている。また、これらの暗号アルゴリズムの計算に必要な多倍長整数演算機能も含まれている。ASF01 の機能に関しては、5.1 節に概要を記載する。
Core モジュール用設定ファイル		Core モジュールの動作設定を記述するテキストファイル。Core モジュールそのものの動作を設定するファイルと、読み込むアルゴリズムプラグインを定義するためのファイルから成る。
公開鍵ファイル		JCATT の完全性・不正改造検出機能の実装のために使用する公開鍵。署名検証のために使用する。
秘密鍵ファイル		JCATT の完全性・不正改造検出機能の実装のために使用する公開鍵。署名生成のために使用する。IPA のみが使用する。
プロジェクトファイル		プロジェクトの状態を保存するファイル。詳細は 4.1.5 節を参照。

セットアップツール	JCATT の完全性・不正改造検出機能の実装のために、RSASSA-PSS による署名生成を行って署名ファイルを生成する独立したプログラム。認証機関のみが使用する。
-----------	--

表1: JCATT3 の構成

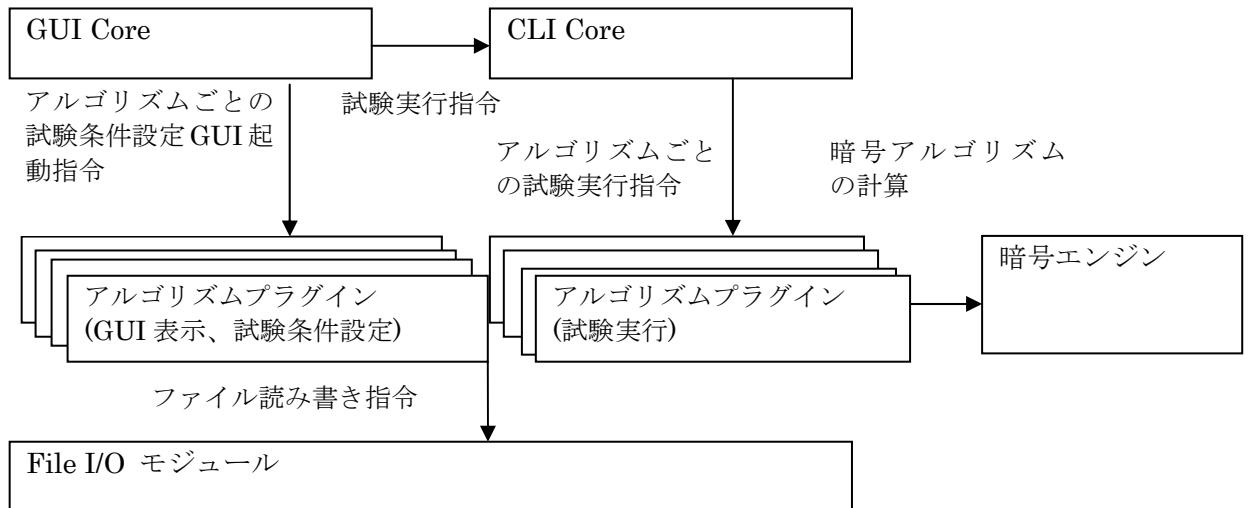
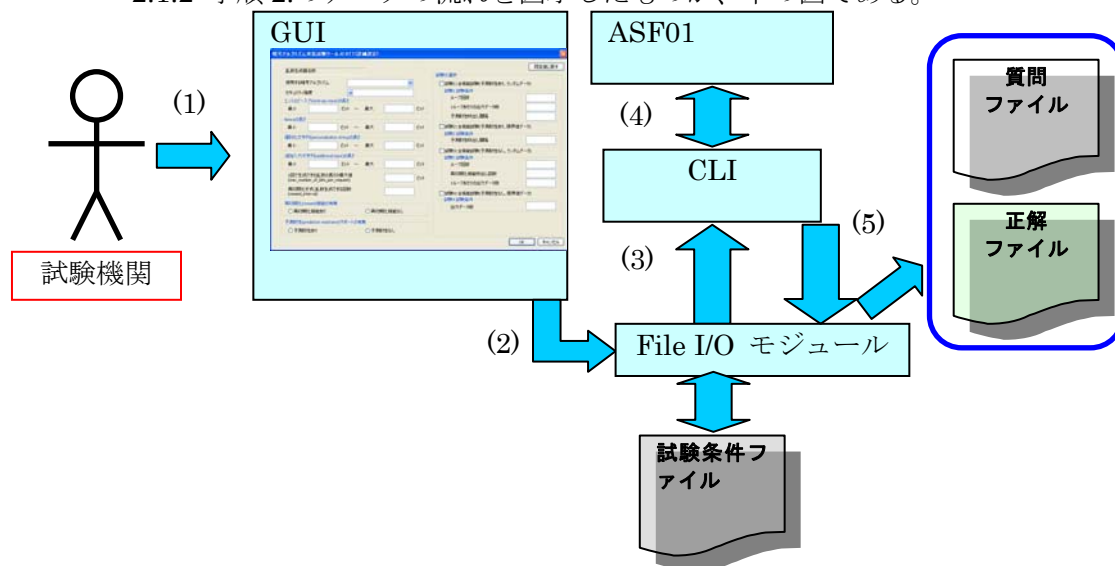


図 1: JCATT3 のモジュール構成

2.2.2. JCATTの構成ファイルとデータの流れ

2.2.2.1. 質問ファイル及び正解ファイル生成時

2.1.2 手順 2.のデータの流れを図示したものが、下の図である。

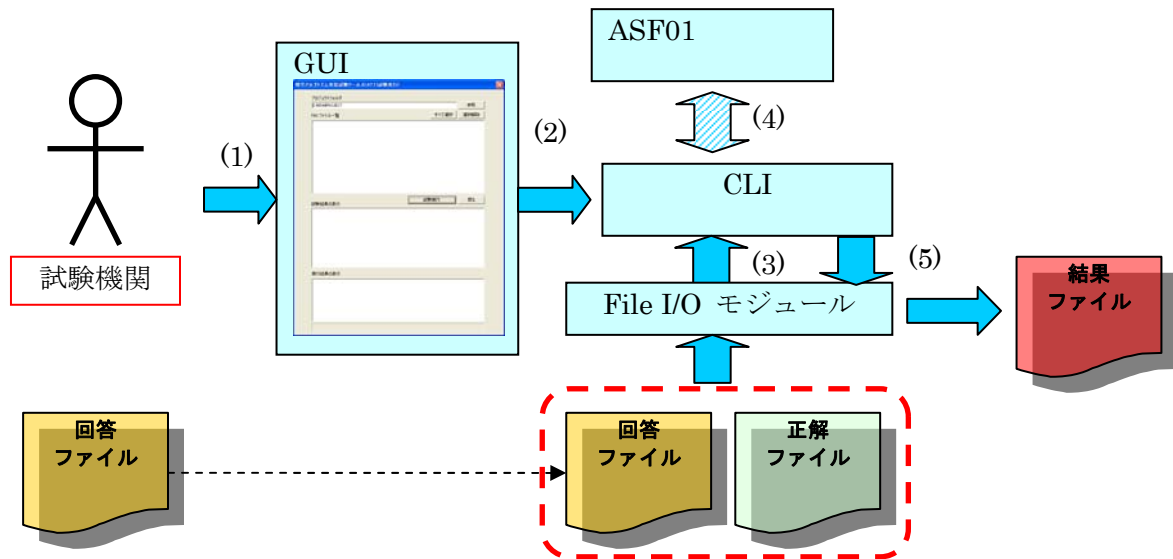


図中の(1)～(5)の説明は、以下の通りである。

- (1)画面から試験条件を入力する。
- (2)画面から入力された試験条件をプロジェクトファイルに出力する。
- (3)CLI がプロジェクトファイルに記載された試験条件を読み込む。
- (4)試験条件を元に、試験パターンに基づく入力データを ASF01 を用いて生成する。
- (5)(4)の試験パターンに基づく質問ファイル及び正解ファイルを出力する。

2.2.2.2. 試験実行時

2.1.2 手順 5.のデータの流れを図示したものが、下の図である。



図中の(1)～(5)の説明は、以下の通りである。

- (1) 回答ファイルを入力すると共に、画面から試験を実行する。
- (2) 試験を実行する回答ファイル及び対応する正解ファイルを CLI に指定する。
- (3) 指定された回答ファイル及び対応する正解ファイルを読み込む。
- (4) 試験パターンが既知解テストでない場合、回答ファイルに記載された暗号アルゴリズムの入力データを ASF01 に入力して、回答ファイルに記載された暗号アルゴリズムの出力データが再現できるか検証を行う。
- (5) 試験パターンが既知解テストの場合、回答ファイル及び正解ファイルを比較し、試験結果を結果ファイルに出力する。試験パターンが既知解テストでない場合、(4)で行った検証結果を結果ファイルに出力する。

3. 開発内容

3.1. 開発項目概要

今回の開発項目は以下の 4 項目である。以下の 4 項目の詳細については、「4. 開発機能詳細」および「6. ドキュメント」で記述する。

(1) Core モジュールの開発

(2) JCATT の完全性・不正改造検出機能

(3) アルゴリズムプラグインの作成。サポートするアルゴリズムは以下の通りで、アルゴリズムごとに別個のプラグインとする。

- AES (暗号化及び復号。鍵長は 128 ビット、192 ビット、 256 ビット。利用モードは NIST SP800-38A で定義されたもの)
- RSASSA-PSS (鍵ペア生成、署名作成、署名検証)

(4) 取扱説明書の作成

また、プログラム及びドキュメントは、公開を前提とした整備を行うこと。

3.2. 開発前提条件

今回の開発における前提条件を以下に示す。JCATT3 の構成要素のうち、開発対象であるものと既存のモジュールであるものの一覧は、以下の表のとおりである。

構成要素		新規開発 対象区分	備考
Core モジュール	GUI Core	対象	
	CLI Core	対象	
	File I/O モジュール	対象	
アルゴリズムプラグイン	AES	対象	暗号アルゴリズムそのものの計算に関しては、提供モジュールである ASF01 を使用可能。
	RSASSA-PSS	対象	暗号アルゴリズムそのものの計算に関しては、提供モジュールである ASF01 を使用可能。
暗号エンジン(ASF01)		—	IPA から提供するモジュールである。機能概要に関しては、5.1節を参照。
セットアップツール		対象	暗号アルゴリズムの計算に関しては、提供モジュールである ASF01 を使用可能。

3.3. JCATTの動作環境

開発する JCATT の動作環境は次の通りとする。

- OS : 以下のいずれでも動作すること
 - Microsoft Windows XP Professional SP3 (32 ビット環境、日本語版及び英語版)
 - Microsoft Windows 7 Professional (32 ビット環境及び 64 ビット環境、日本語版及び英語版)
- CPU : Intel Pentium 4 プロセッサまたはその同等品
- RAM : 1024MB 以上

Microsoft Windows 以外の環境(Linux 等)での動作保証は本開発の開発者には課さないが、

Microsoft Windows 環境以外への移植性を考慮した設計とすること。例えば、特定の処理系に依存する C/C++言語の拡張仕様は原則として使用しない、共有ライブラリの動的読み込みを行う場合、LoadLibrary 等の Win32API を直接使用せず、Qt の QLibrary クラスを使用する、といった方法を取ることによって移植性の高いコードを記述すること。Microsoft Windows における動作に問題がない場合であっても、IPA が開発中に Microsoft Windows 以外の環境でのビルドや動作に支障があることを理由にして設計(ソースコードを含む)の修正を要求した場合は、修正要求に応じること。

3.4. JCATTの開発環境

JCATT の開発には Microsoft Visual C++ 2005 あるいは Microsoft Visual C++2010 を使用してコンパイル/リンクを行うこと(IDE は Visual Studio でなくてもよい。例えば、Qt Creator を使用してもよい)。開発言語は C/C++言語を使用すること。ユーザインタフェースの 2 か国語対応(英語/日本語)は、Qt の国際化機能を使用すること。XML ファイルの読み書きは Qt の XML ライブラリを使用すること。ドキュメントとソースコードは構成管理ツールを使用して適切なバージョン管理を行うこと。GUI ツールキットには Qt 4.7.3 以降(LGPL 版)を使用すること。

また、試験は単体テスト用のフレームワーク CppUnit(以下の URL 参照)

<http://sourceforge.net/projects/cppunit/>

あるいは開発会社で規定されている開発・試験手順に基づいて、単体テスト、結合テスト、システムテストを実施すること。

4. 開発機能詳細

4.1. Coreモジュールの開発

JCATT3 を、表 1に挙げるモジュールの組み合わせとして構成する。暗号エンジン以外はすべて新規のプログラムである。

各モジュールの詳細については、以下の節に記載する。

4.1.1. Coreモジュール用設定ファイル

GUI Core、CLI Core、File I/O モジュールを合わせて Core モジュールと呼ぶ。Core モジュールの動作を規定するために、以下の設定ファイルを使用する。

(1) `jcatt.conf`

JCATTが読み込むファイルのディレクトリ、言語設定、乱数シードについての設定、ファイルフォーマットの指定、完全性・不正改造検出機能のための公開鍵のファイル名、アルゴリズムプラグイン設定ファイルのファイル名、アルゴリズムプラグイン設定ファイルで使用する文字コード¹についての設定を行う。アルゴリズムプラグイン設定ファイルのファイル名については、可変部分を設けて言語コード²を埋め込めるようにする(例えば、英語の場合には”`plugins_en.conf`”、日本語の場合には”`plugins_ja.conf`”のようにする)。

(2) アルゴリズムプラグイン設定ファイル(ファイル名は `jcatt.conf` で指定)

組み込むアルゴリズムプラグインを設定する。サポートするアルゴリズムの分類も含めて定義する。アルゴリズム名や分類名には英語だけでなく日本語も使用できる。1 個のアルゴリズムプラグインが複数のアルゴリズムをサポートすることも可能とする。

設定ファイルの書式については、人間が直接エディタで編集することを想定して設計すること。

4.1.2. GUI Coreの機能詳細

GUI Core は、以下の機能を有するものとする。

- (1) メニューバーを有するメインウィンドウベースの GUI アプリケーションである。
- (2) 完全性・不正改造検出機能を持つ。詳細については、4.2.2節(署名検証機能)を参照。
- (3) ウィンドウタイトルには、”[プロジェクト名]・JCATT [バージョン番号]”と表示する。プロジェクトを読み込んでいない状態では、[プロジェクト名]には何も表示しない。
- (4) ユーザインタフェースは、日本語及び英語での表示が可能である。言語の切り替え機構は、Qt の国際化機能を使用して実装する。つまり、GUI は英語で作成し、それに対応する日本語の翻訳ファイル(.qm)を作成し、Qt のリソースとして実行ファイルに取り込むことにより、日本語表示を選択した場合はその翻訳ファイルをロードする方式とする。言語はユーザ選択可能で、起動時に設定ファイルによって決定できるようにすること。実行中の動的な言語切り替えをサポートしてもよい。
- (5) 使用するアルゴリズムプラグインは、Core モジュール用設定ファイルに指定する。アルゴリズムプラグインを呼び出すための取り決めも設計すること。
- (6) 起動時に、「プロジェクト情報」「ファイル生成」「試験実行」「試験結果の表示」の 4 個のタブからなるタブウィジェット及び終了ボタンを表示したダイアログを表示する。
- (7) 「プロジェクト情報」以外のタブには、アルゴリズム一覧表示エリアを表示させる。アルゴリズム一覧表示エリアには、アルゴリズムプラグインによって使用可能になっているア

¹ 文字コードの指定は、IANAで定義されたcharacter set名で行う。動作確認は、少なくともISO 8859-1, Shift_JIS, UTF-8 に対して行うこと。不正な文字コード名のチェックはQtに任せ、前述の動作確認対象以外の文字コード名をはじく処理を独自に作り込まないこと。

² ISO 639-1 の 2 文字の言語コードを使用する。

ルゴリズムを、分類に従った階層構造で表示する。また、各アルゴリズムに対して、定義済みの試験条件をアルゴリズム名の下位階層に表示する。

- (8) 「ファイル生成」タブには、アルゴリズム一覧表示エリアに加えて、「ファイル生成」ボタン、メッセージ表示エリアを表示する。
- (9) 「ファイル生成」タブのアルゴリズム一覧表示エリアに表示されている個別のアルゴリズムには、試験対象かどうかを指定するチェックボックスを表示する。定義済み試験条件はクリック可能で、クリックするとアルゴリズムプラグインの試験条件設定エントリを呼び出して試験条件設定画面を表示する。また、各アルゴリズム名に対して「新規試験条件の作成」を可能とする。クリック可能な文字列には下線を引き、クリック可能な文字列の上にマウスカーソルが移動した場合にはクリック可能であることを示す形状に変化させる。試験条件は1個のアルゴリズムに対して複数定義することができる。
- (10) 「ファイル生成」タブからは、新規の試験条件の作成、定義済み試験条件の編集、定義済み試験条件の削除、
- (11) 「ファイル生成」タブの「ファイル生成」ボタンを押下すると、選択された試験条件に対応する質問ファイル、正解ファイルを、CLI を起動することによって生成する。
- (12) 「試験実行」タブには、アルゴリズム一覧表示エリアに加えて、「試験実行」ボタン、メッセージ表示表示エリアを表示する。
- (13) 「試験実行」タブのアルゴリズム一覧表示エリアに表示する定義された試験条件の中で、試験実行が可能でないもの(対応する回答ファイルがないもの)についてはグレー表示とする。
- (14) 「試験実行」タブの「試験実行」ボタンを押下すると、選択された試験条件に対する暗号アルゴリズム実装試験を、CLI を起動することによって実行する。実行後には、各試験条件に対して、少なくとも全体としての合否情報をメッセージ表示エリアに表示する。
- (15) 「試験結果表示」タブには、アルゴリズム一覧表示エリアに加えて、「結果表示」ボタンを表示する。
- (16) 「試験結果表示」タブのアルゴリズム一覧表示エリアに表示する定義された試験条件の中で、試験結果が存在するもの(対応する結果ファイルがあるもの)以外についてはグレー表示とする。
- (17) 「試験結果表示」タブの「試験結果表示」ボタンを押下すると、選択された試験条件に対する暗号アルゴリズム実装試験の結果ファイルの内容を表示する。
- (18) メニューバーからは、少なくとも以下の操作が行える。

メニュー	サブメニュー	機能
ファイル	新規プロジェクト	プロジェクトの新規作成
	プロジェクトを開く	既存のプロジェクトを読み込む
	プロジェクトを保存	現在のプロジェクトを上書き保存する
	名前をつけてプロジェクトを保存	現在のプロジェクトを、ファイルダイアログを表示させてファイル名を指定させてファイルに保存する。
	終了	JCATT を終了する。
ヘルプ	JCATT について	JCATT のバージョン情報を表示する。
	プラグインについて	組み込まれているアルゴリズムプラグインの情報を表示する

ヘルプメニューは、Motif スタイル、CDE スタイルでは右端に表示する。

- (19) 画面の最下部には、全体の進捗状況を示すプログレスバーを表示する。
- (20) プロジェクトに関する機能については、4.2節を参照。
- (21) 起動時にコマンドライン引数が指定された場合、第1引数をプロジェクトファイルのマスター名とみなし、起動と同時にファイルをプロジェクトファイルとして読み込む。
- (22) GUI の設計にあたっては、多数のアルゴリズムを試験する場合であっても、極力少ない操作回数で済むような設計を行うこと(階層の全展開、全選択、指定した項目の下位階層の一括選択の操作を設ける等)。

(23) GUI の動作中に回答ファイル等が作成あるいは削除されることも考慮し、適切なタイミングでの状態の更新を行う仕組みも設計すること。

参考までに、JCATT3 のGUI画面のプロトタイプ(日本語表示時)を図 2～図 5に示す。これらはプロトタイプであり、最終的な仕様は基本設計で確定させる。

The screenshot displays the JCATT 3.0.0 application window. The title bar reads 'JCATT 3.0.0'. Below the title bar is a menu bar with 'ファイル(F)' and 'ヘルプ(H)'. The main area features a tabbed interface with four tabs: 'プロジェクト情報' (selected), 'ファイル生成', '試験実行', and '試験結果表示'. Under the 'プロジェクト情報' tab, there are two sections: 'ベンダ情報' and '実装情報'. The 'ベンダ情報' section contains a table with the following fields: 会社名, 郵便番号, 住所1, 住所2, 担当者, Eメールアドレス, 部署, 電話, and FAX番号. The '実装情報' section contains a table with the following fields: 実装名, バージョン, and 動作環境. A '終了' button is located in the bottom right corner of the window.

ベンダ情報	
会社名	
郵便番号	
住所1	
住所2	
担当者	
Eメールアドレス	
部署	
電話	
FAX番号	

実装情報	
実装名	
バージョン	
動作環境	

図 2: プロジェクト情報タブ表示



図 3: ファイル生成タブ表示

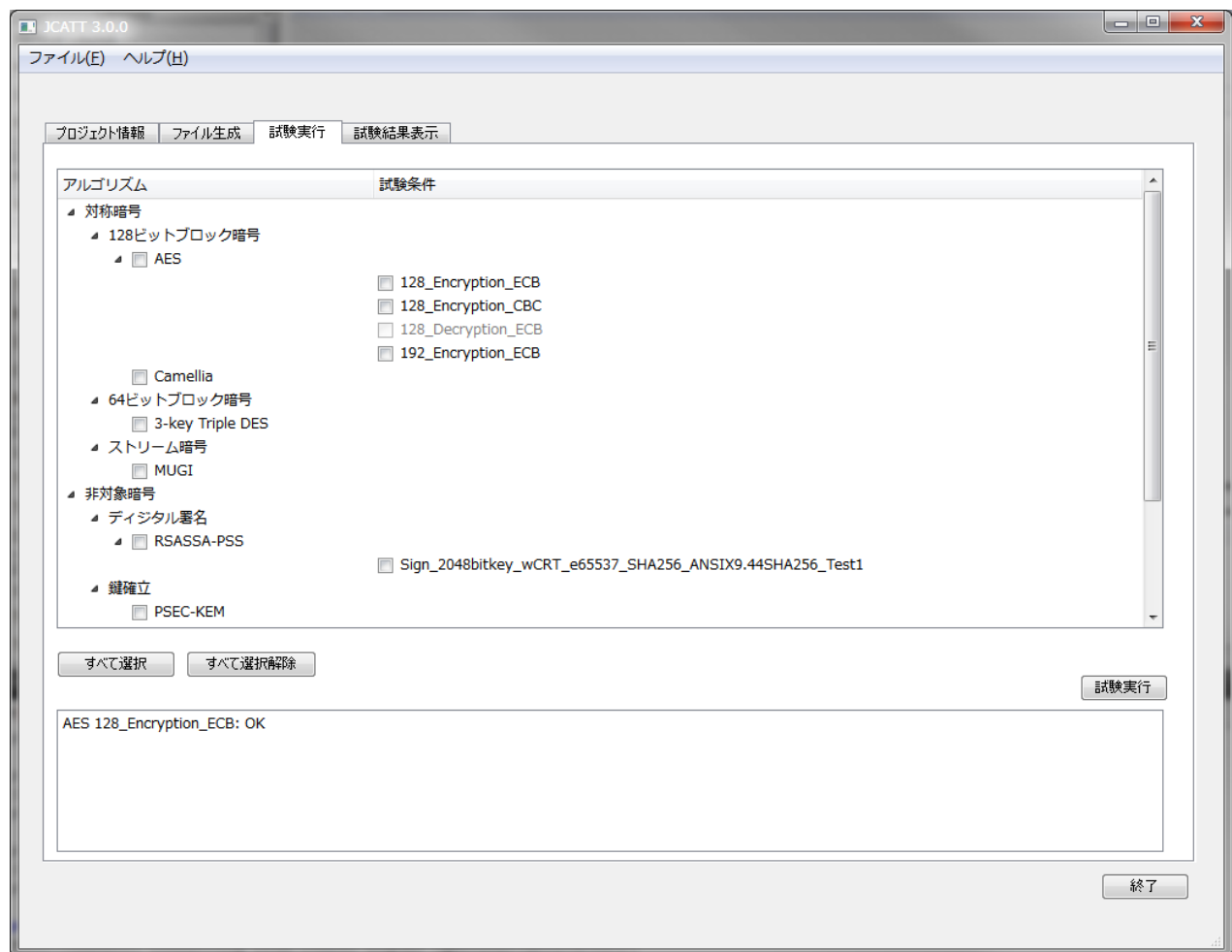


図 4: 試験実行タブ表示

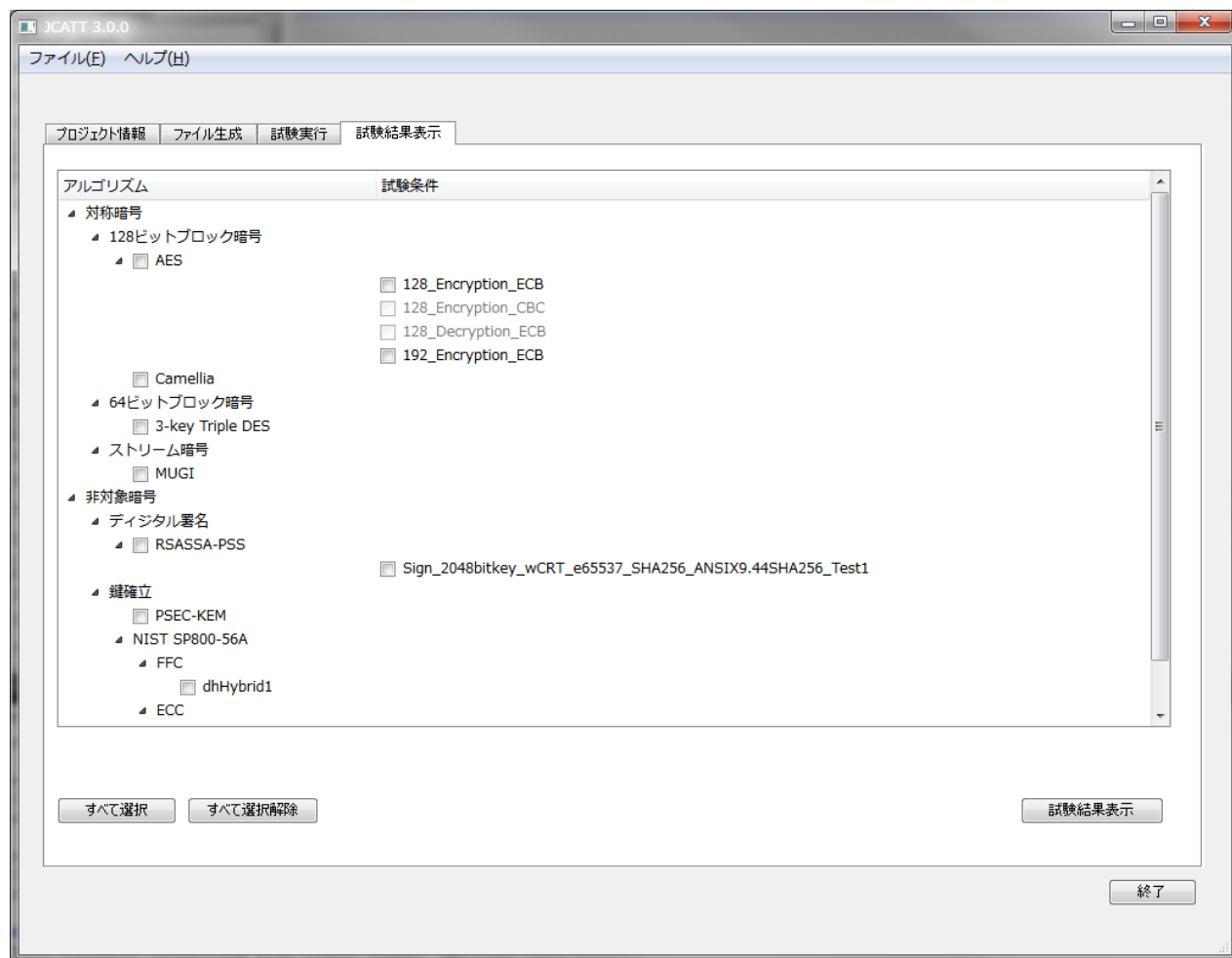


図 5: 試験結果表示タブ表示

4.1.3. CLI Coreの機能要件

CLI Core は、以下の機能を有するものとする。

- (1) CLI アプリケーションである。
- (2) 出力メッセージは英語である。
- (3) ファイル生成機能、試験実行機能を持つ。どちらの機能を実行するかは、コマンドラインオプションで指定する。
- (4) ファイル生成機能では、試験条件ファイルから各アルゴリズムの試験条件を読み込み、対応したアルゴリズムプラグインをロードし、ファイル生成機能エントリを呼び出してファイル生成を行う。アルゴリズムプラグインを呼び出すための取り決めも設計すること。
- (5) 試験実行機能では、試験条件ファイルから各アルゴリズムの試験条件を読み込み、対応したアルゴリズムプラグインの試験実行機能エントリを呼び出してファイル生成を行う。

4.1.4. File I/Oモジュールの機能要件

File I/O モジュールは、少なくとも以下の機能を有するものとする。

- (1) 質問ファイル、正解ファイル、回答ファイルの内容を抽象的なデータ構造として受け取り、

- (2) JCATT2 フォーマットあるいは CAVS フォーマットの質問ファイル、正解ファイル、回答ファイルの内容を読み込んで解析し、抽象的なデータ構造として提供する API を持つ。
- (3) プロジェクトファイル群の読み込み及び書き出し

JCATT2 と CAVS のどちらのファイルフォーマットを採用するかは、Core モジュール用設定ファイルで指定する。

JCATT2 フォーマットの仕様については、「JCATTファイルフォーマット仕様書」を参照すること。CAVSのファイルフォーマットについては、NISTのTest Vector³を参照すること。出力されるファイルには、JCATT 及びアルゴリズムプラグインのバージョン番号(署名検証に失敗している場合には、その旨を表す情報)を先頭部分にコメントとして挿入すること。

4.1.5. プロジェクト機能についての詳細

プロジェクトは、以下のファイル群からなる。

種別	内容
マスターファイル	プロジェクトを定義する最上位ファイル。プロジェクト名、プロジェクトの状態(画面表示状態、試験対象として選択したアルゴリズムの情報を含む)、プロジェクトで使用する試験条件ファイル名、IUT 情報ファイル名を保持する。
試験条件ファイル	暗号アルゴリズム実装試験の試験条件を保存するファイル。試験対象のアルゴリズムごとに 1 個以上作成される。
IUT 情報ファイル	IUT に関する情報を定義する XML ファイル。ベンダ情報(ベンダ名、郵便番号、住所、担当者、部署、電話番号、FAX 番号)、IUT 情報(暗号実装名、バージョン情報、動作環境(マシン名、CPU、メモリ、OS 等)を含む。

以上を総称して、プロジェクトファイル群と呼ぶ。

プロジェクトの新規作成時には、プロジェクトのマスターファイルのファイル名およびディレクトリをファイルダイアログで指定できる画面を表示する。

IUT 情報は、プロジェクト情報タブから編集できる。

プロジェクトの読み込み時には、マスターファイル及びそれから参照されているファイル群を読み込み、IUT に関する情報、試験条件、プロジェクトの状態を設定する。IUT に関する情報の設定は、プロジェクト情報タブの入力領域に反映することで行う。

アプリケーション終了時に、試験情報あるいは IUT に関する情報に未保存の項目がある場合、保存するかどうかを確認するダイアログを表示し、必要に応じてプロジェクト情報を保存する。

4.2. JCATTの完全性・不正改造検出機能

暗号アルゴリズムを用いた完全性確認技術であるデジタル署名を使用して、本試験ツールの完全性の確認及びその不正改造を検出する機能を実装すること。

4.2.1. 署名生成機能

署名生成機能を実現するため、以下の機能を実装したセットアップツールを作成すること。

- (1) CLI アプリケーションである。
- (2) RSA 暗号の鍵ペア(鍵のビット長は 1024 以上 8192 以下かつ 512 の倍数、デフォルトは 2048)を生成し、公開鍵と秘密鍵をそれぞれファイルに出力する。
- (3) 表 2 の情報を入力メッセージとして、RSASSA-PSSアルゴリズムによるデジタル署名

³ <http://csrc.nist.gov/groups/STM/cavp/index.html>

(Coreモジュールに対する署名)を生成し、ファイルに出力する。署名生成用の秘密鍵のファイル名とMACアドレスはコマンドラインから入力する。MACアドレスは、16進表記した各オクテットを”-“あるいは”:"で区切った表記で入力する。

読み込み順序	情報	属性
1	GUI Core の実行ファイル	バイナリファイル
2	CLI Core の実行ファイル	バイナリファイル
3	File I/O モジュールのファイル	バイナリファイル
4	ASF01 の共有ライブラリファイル	バイナリファイル
5	PC の MAC アドレス	6 バイトのバイナリデータ

表 2: Core モジュールに対する署名の対象となる入力情報

- (4) アルゴリズムプラグイン設定ファイル(4.1.1の(2))を読み込み、各アルゴリズムプラグインのファイルの内容に対するRSASSA-PSSアルゴリズムによるデジタル署名(プラグインに対する署名)の一覧を生成し、ファイルに出力する機能を持つ。署名生成用の秘密鍵のファイル名と、アルゴリズムプラグイン設定ファイル名はコマンドラインから入力する。
- (5) C/C++の標準ライブラリ以外で直接使用してよいライブラリは、Qt、ASF01 のみとする。

4.2.2. 署名検証機能

署名検証機能を実装するために、GUI Core に以下の処理を実装すること。

- (1) 表 2に記載した情報を入力メッセージとして、Core用設定ファイルに記載した公開鍵を使用して署名検証を行う。署名検証に失敗した場合は、エラーメッセージを出力してGUI Coreは強制終了する。
- (2) アルゴリズムプラグイン組み込み時には、各プラグインについてプラグインに対する署名を検証する。署名検証に失敗した場合には、当該プラグインの署名検証に失敗したことを通知するメッセージを表示する。この場合、ヘルプメニューから表示されるプラグイン情報には、署名検証に失敗したことを示す情報を表示する。

4.3. アルゴリズムプラグインの作成

アルゴリズムプラグインは、Core モジュールから呼ばれるため、Core モジュールとプラグインとの間の呼び出し規約に従い、少なくとも以下の機能を実装する必要がある。

機能	詳細
試験条件設定	試験条件設定のための GUI を起動し、設定された条件を試験条件ファイルに書き込む。
試験実行	試験条件ファイルから試験条件を読み込み、試験を実行する
バージョン情報	プラグインのバージョン情報を返す。

試験仕様は、「暗号アルゴリズム実装試験仕様書」に従う。このため上記の「試験条件設定」及び「試験実行」機能は、「暗号アルゴリズム実装試験仕様書」で規定される各種アルゴリズム、およびパラメータの調査検討をしたうえで機能を設計開発すること。

本開発においては、AES の試験機能を実現するためのアルゴリズムプラグイン及びRSASSA-PSS の試験機能を実現するためのアルゴリズムプラグインを作成する。

アルゴリズムプラグインの実装にあたっては、以下の注意事項を守ること。

- (1) 試験条件設定画面には、最低限以下のウィジェットを配置すること。
 - 試験条件名を入力する入力エリア。生成されるファイルのファイル名のプレフィック

スとして使用する。

- ファイル名(拡張子を除いた部分)を表示する、読み込み専用の入力エリア。内容は、試験条件名、試験条件から自動生成される。ファイル名は、ASCII 印字可能文字で構成され、Microsoft Windows のファイルシステムで使用できない文字、及び空白文字を含まないようにすること。
- 試験条件の各パラメータについては、適切なエラーチェックを行い、「暗号アルゴリズム実装試験仕様書」の条件を満たさないパラメータが入力されて保存されようとした場合には適切なエラーメッセージを出力してはじくこと。なお、ある特定の文字種のみが正しい入力のなり得るような場合(例えば、10 進数値の入力領域においては”0”～”9”の数字のみが正しい入力文字である)、入力段階で正当でない文字の入力を禁止してもよい。
- 以下の機能を持つボタン群。QDialogButtonBox クラスを使用して実装する。画面の下部に、水平に並べて配置する。

英語ラベル	日本語ラベル	機能
Restore Default	既定値に戻す	試験条件の入力値を既定値に戻す
OK	OK	試験条件を保存して GUI を終了する
Save	保存	GUI を終了せずに試験条件を保存する。
Cancel	キャンセル	試験条件を保存せずに GUI を閉じる

GUIのプロトタイプを、図 6に示す。

- (2) 乱数を使用する場合には、ASF01 に実装されている「NIST SP800-90 に基づく疑似乱数生成器」を使用すること。
- (3) GUI は英語で作成し、日本語の翻訳ファイルを作成して Qt のリソースとして取り込むことによって英語表示と日本語表示を選択可能とすること。言語の選択は、GUI Core と同じとする。
- (4) QUiLoader クラスによるダイアログの動的生成機能を使用しないこと。

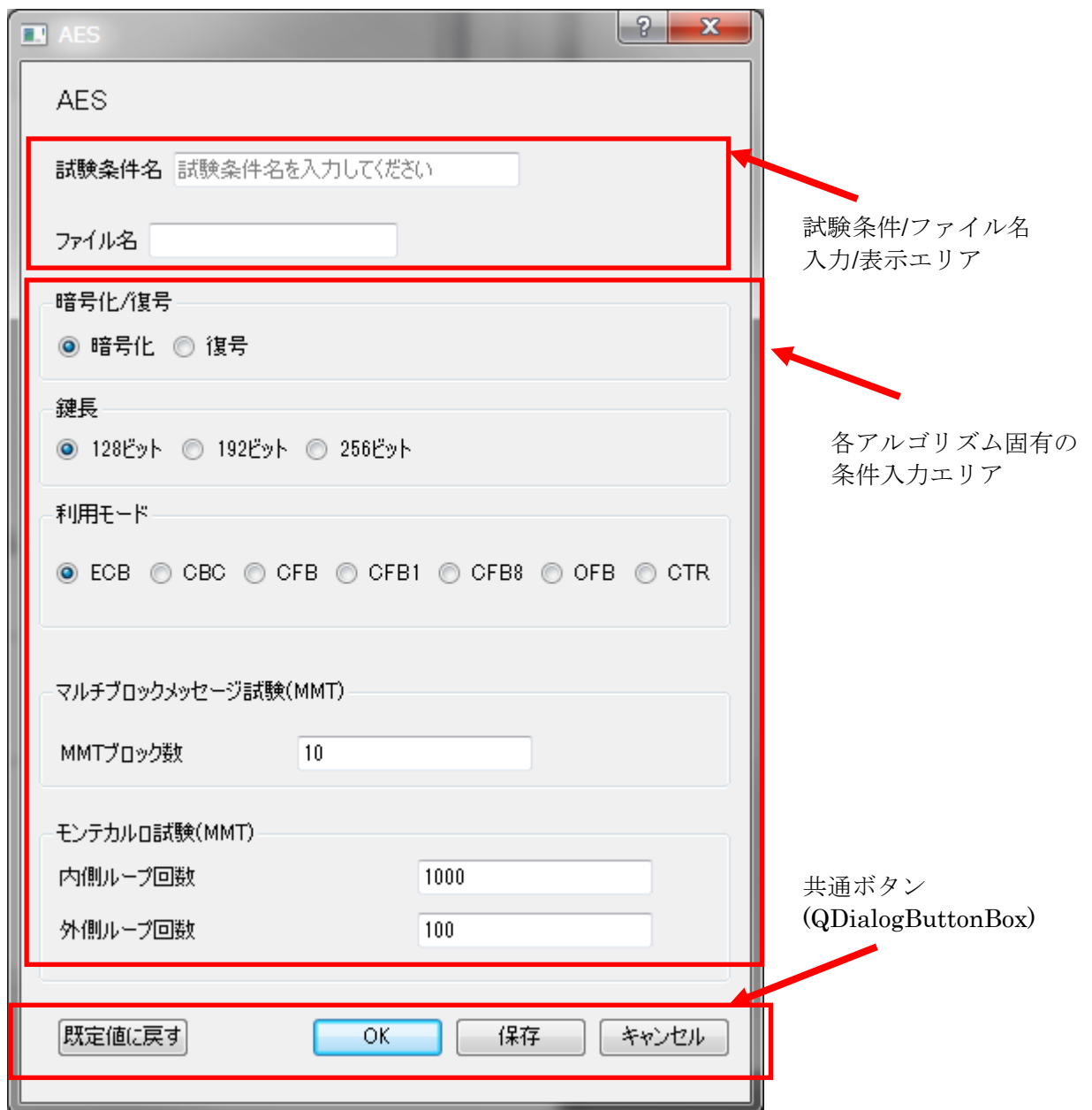


図 6: 試験条件設定画面のプロトタイプ

4.3.1. AES試験機能

AES の暗号アルゴリズム実装試験仕様は、「暗号アルゴリズム実装試験仕様書 – 共通鍵 –」(ATR-01-B)に定義されている。

AES においては NIST SP800-38A で定義されている暗号の利用モード、すなわち ECB, CBC, CFB1, CFB8, CFB, OFB, CTR に対して、それぞれ暗号化と復号の試験をサポートする。試験機能の実装にあたっては、アルゴリズムそのものの計算(利用モードを含む)は ASF01 に実装されているものを使用する。

4.3.2. RSASSA-PSS試験機能

RSASSA-PSS の暗号アルゴリズム実装試験仕様は「暗号アルゴリズム実装試験仕様書 – 公開鍵 –」(ATR-01-A)に定義されている。

RSASSA-PSSにおいては、鍵ペア生成、署名生成、署名検証の試験をサポートする。試験機

能の実装にあたっては、ASF01 に実装されている鍵ペア生成機能⁴、署名生成機能、署名検証機能、多倍長整数演算機能を使用して実装する。

⁴ ASF01 に実装されているRSA鍵ペア生成は、厳密にはFIPS186-3 の仕様を満たさないが、FIPS186-3 仕様の鍵生成機能は本開発の開発対象には含めない。

5. 参考資料

5.1. ASF01 の機能

暗号ライブラリ ASF01 は、様々な暗号アルゴリズム、及びそれらの計算を行うための基礎的な数学関数をサポートしている。ASF01 がサポートしている機能には、以下のものが含まれる。

- 多倍長整数演算。任意の長さの非負整数の加算、減算、乗算、除算、除算剰余、べき乗剰余、比較、最大公約数の計算、Miller Rabin 法による確率的素数判定を含む。
- AES 暗号の暗号化及び復号。
- ブロック暗号の利用モード。ECB、CBC、CFB、CFB1、CFB8、OFB、CTR がサポートされる。これらの利用モードを AES 暗号化/復号と組み合わせることができる。
- RSA 鍵生成
- RSASSA-PSS 署名生成/署名検証
- SP800-90に基づく疑似乱数生成器のうち、Hash_DRBG、HMAC_DRBG、CTR_DRBG。

5.2. JCATT2 の試験条件設定画面(参考)

本章では、参考資料として、JCATT2 における試験条件設定画面を掲載する。これはあくまで参考資料であり、JCATT3 の試験条件設定画面の仕様をこれと同一にすることを意味しない。

5.2.1. AES

JCATT2 における AES(128 ビット鍵、ECB暗号化)の試験機能設定画面は、図 7の通りである。

The screenshot shows a window titled "暗号アルゴリズム実装試験ツールJCATT(詳細設定)". Inside, the selected test is "AES - 128 bit key - ECB_Encryption". There is a button "既定値に戻す" (Reset to default). The settings are as follows:

- 種々の平文に対する既知入出力試験(KAT-Text)
- 種々の鍵に対する既知入出力試験(KAT-key)
- マルチブロックメッセージ試験(MMT)
 - MMTブロック数: 10
- モンテカルロ試験(MCT)
 - MCT
 - 内側ループ回数: 1000
 - 外側ループ回数: 100
- GFSbox 既知入出力試験(KAT-GFSbox)
- KeySbox 既知入出力試験(KAT-KeySbox)

At the bottom, there are buttons "保存" (Save) and "戻る" (Back).

図 7: JCATT2 の AES の試験条件設定画面(参考)

5.2.2. RSASSA-PSS

JCATT2 における RSASSA-PSS の試験条件設定画面は、図 8～図 10 の通りである。

The screenshot shows a window titled "暗号アルゴリズム実装試験ツールJCATT(詳細設定)". Inside, the "RSA-PSS - Key Generation" section is active. It includes a "既定値に戻す" button. The "鍵長" (Key Length) is set to "1024" bits. Under "プライベート鍵のタイプ選択" (Private Key Type Selection), the "CRTあり(p, q, dP, dQ, qInv)" option is selected. Under "公開鍵 e のタイプ選択" (Public Key e Type Selection), the "65537" option is selected. The "生成回数" (Number of Generations) is set to "10" items. At the bottom, there are "保存" (Save) and "戻る" (Back) buttons.

図 8: JCATT2 の RSASSA-PSS の 鍵ペア生成試験条件設定画面(参考)

暗号アルゴリズム実装試験ツールJCATT(詳細設定)

RSA-PSS - Sign 既定値に戻す

鍵長 ビット

プライベート鍵のタイプ選択

- ☒ CRTあり($p, q, dP, dQ, qInv$)
- ☐ CRTなし(n, d)

公開鍵 e のタイプ選択

- ☒ 65537
- ☐ ランダム

平文のビット長 ビット

平文の数 個

ハッシュ関数

MGF関数

saltのビット長 ビット

試験の選択

- ☒ 試験1: Random Generation Test (ランダムな平文に対するテスト)
いつも異なる署名が生成されることを検証するための署名の個数 個
- ☐ 試験2: Known Answer Test (疑似乱数生成関数および乱数シードを指定)
- ☐ 試験3: Known Answer Test (saltを指定)

保存 戻る

図 9: JCATT2 の RSASSA-PSS の 署名作成試験条件設定画面(参考)

暗号アルゴリズム実装試験ツールJCATT(詳細設定)

RSA-PSS - Verification 既定値に戻す

鍵長 ビット

プライベート鍵のタイプ選択

- ☒ CRTあり(p, q, dP, dQ, qInv)
- ☐ CRTなし(n, d)

公開鍵 e のタイプ選択

- ☒ 65537
- ☐ ランダム

平文のビット長 ビット

平文の数 個 改ざんデータのパーセント %

ハッシュ関数

MGF関数

saltのビット長 ビット

保存 戻る

図 10: JCATT2 の RSASSA-PSS の署名検証試験条件設定画面(参考)

5.3. 参考文献

本プログラムを開発するにあたっての参考文献を以下に挙げる。なお、この参考文献から参照されている別の文献が、その内容を補完している場合がある。

- 暗号アルゴリズム実装試験仕様書 — 公開鍵 — (ATR-01-A)
<http://www.ipa.go.jp/security/jcmvp/documents/atr/atr01a.pdf>
- 暗号アルゴリズム実装試験仕様書 — 共通鍵 — (ATR-01-B)
<http://www.ipa.go.jp/security/jcmvp/documents/atr/atr01b.pdf>
- JCATT ファイルフォーマット仕様書
http://www.ipa.go.jp/security/jcmvp/documents/open/jcatt/format/jcatt_fileformat_a.zip
<http://www.ipa.go.jp/security/jcmvp/documents/open/jcatt/format/jc>

- NIST SP800-38A
Recommendation for Block Cipher Modes of Operation
<http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf>
- NIST SP800-90
Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)
http://csrc.nist.gov/publications/nistpubs/800-90/SP800-90revised_March2007.pdf
- PKCS#1 v2.1
RSA Cryptography Standard
<ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf>
- FIPS PUB 186-3
Digital Signature Standard (DSS)
<http://csrc.nist.gov/publications/fips/fips186-3/fips186-3.pdf>
- FIPS PUB 197
ADVANCED ENCRYPTION STANDARD (AES)
<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
- NIST Cryptographic Algorithm Validation Program (CAVP)
(CAVS で入出力されるファイルフォーマットに従った text vectors が公開されている)
<http://csrc.nist.gov/groups/STM/cavp/index.html>

6. ドキュメント

6.1. 基本設計書

基本設計書は、少なくとも以下の内容を含むこと。

- 全体で実現する機能を記載すること。
- 各ソフトウェア構成要素がその機能をどのように実現しているかをファイル単位で明確化していること。
- 各ソフトウェア構成要素を使用するにあたっての制約条件を明確化すること。

6.2. 詳細設計書

詳細設計書は、少なくとも以下の内容を含むこと。

- 実現する各機能に対して、その仕様を各ソフトウェア構成要素単位で記述すること。

6.3. 取扱説明書

JCATT 及び各アルゴリズムプラグインの取扱説明書を新規に作成すること。説明書の言語は日本語とする。取扱説明書には、以下の内容を含むこと。

- 試験機関が JCATT を使用して暗号アルゴリズム実装試験を実行するために必要な手順。アルゴリズムプラグインの組み込み方法を含む。
- 各アルゴリズムプラグインに関する、サポートされた暗号アルゴリズムの実装試験の手順。
- アルゴリズムプラグインの開発方法の説明。JCATT の内部構造を知らず、初めてアルゴリズムプラグインを作成する人であっても容易に理解可能な水準の説明とすること。

セットアップツールの取扱説明書を新規に作成すること。説明書の言語は日本語とする。

取扱説明書のファイルフォーマットは、Microsoft Office Word 形式とすること。

7. テスト

開発作業中または作業後にテストを行い、発見された問題について対応し解消すること。テストにあたっては、検証方法、指標、目標値に関して効果的かつ効率的な方針を立案すること。発見された問題及びそれに対応する作業の管理方針についても、プロジェクト計画に含めて立案すること。

- テスト計画を立案し、納入前に適切なテストを実施すること。
- IPA は、少なくとも以下のテストが実施されることを想定している。これによらない場合には、IPA と協議すること。
 - 詳細設計に基づく単体テスト
 - 基本設計に基づく結合テスト
 - 発注仕様に基づくシステムテスト
 - 同値分割、境界値分析の手法を用いた正常系および異常系のテスト。
- 画面のテストにおいては、すべての入力パラメータに対する入力値チェックが機能することのテストを行うこと。

8. 事業の実施体制

- (1) 実施要員に、少なくとも本仕様書の用語集に含まれる各暗号アルゴリズムに精通している者を含めること。本プロジェクトの履行にあたっては、開発担当者に対する、暗号アルゴリズムに精通している者による指導体制を確立すること。
- (2) PMBOK、EVM に基づいたプロジェクト管理等により、作業計画を明確に定め、作業項目毎の工程管理を行い、進捗状況を定期的に IPA 担当者に報告すること。また、作業の遅延等が生じた際には速やかに IPA 担当者に報告すること。

9. 事業期間及びスケジュール

(1) 事業期間

契約締結日から 2012 年 3 月 16 日まで

(2) スケジュール

作業計画の詳細については、契約締結後に別途 IPA と相談の上、IPA が承認するものとする。

10. 検収関連事項

10.1. 納入期限

納入期限は、2012 年 3 月 16 日とする。

10.2. 納入場所

東京都文京区本駒込二丁目 28 番 8 号

独立行政法人情報処理推進機構 技術本部セキュリティセンター

10.3. 納入物件

- 以下記載の文書等を収めた記録媒体(CD-R 又は DVD-R)一式
 - ① 取扱説明書
 - ② テスト報告書、障害管理表（障害内容と対処内容の一覧表）
 - ③ 設計資料（基本設計書、詳細設計書）
 - ④ 納入物件一覧リスト及びソースコード一覧リスト
 - ⑤ JCATT(アルゴリズムプラグインを含む)のソースコード及び実行形式生成に必要なファイル。単体テスト用のソースコードも含む。
 - ⑥ JCATT(アルゴリズムプラグインを含む)の実行用ロードモジュール及び必要な共有ライブラリのファイル。プログラムを動作させるために必要な設定ファイルを含む。
 - ⑦ JCATT 開発成果報告書及びその概要版
- 上記資料①～④、⑦の紙媒体各 1 部を検収用として添付すること。

(3) 納入物件作成にあたっての注意事項

①の作成にあたっては、次の点に留意すること。

- 用語の定義は、「暗号モジュール試験及び認証制度の基本規程（JCM-01）」（<http://www.ipa.go.jp/security/jcmvp/documents/jcm01.pdf>）による。
- 一般的に使用されている用語及び「暗号モジュール試験及び認証制度の基本規程（JCM-01）」において定義されている用語以外の用語を使用する際には、用語の定義を行い、その意味が明確になるように記述すること。

②の作成にあたっては、次の点に留意すること。

- テスト報告書は、十分なテスト項目とそのテスト内容、テスト手順及び判断基準の詳細を記述した文書であること。テストの手法、結果についても報告書に記載すること。
- 障害管理表には、テスト工程において発生した障害内容と、それに対する対処内容を具体的に記述すること。

⑦の作成にあたっては、次の点に留意すること。

- 本開発における成果の概要を簡潔に説明できる文書であること。内容、分量については、過去の情報セキュリティ対策事業に関する開発成果報告書、成果概要報告書と同等以上のものとする（<http://www.ipa.go.jp/security/develop/software.html> を参照）。

記録媒体の作成にあたっては、次の点に留意すること。

- ファイル名には、ASCII あるいは JIS X0208 で定義されている文字集合に属さない文字を使用しないこと。

10. 4. 検収条件

検収では、本仕様書の条件、項目が満たされているか否かにつき確認を行う。また、品質については、実際の暗号アルゴリズム実装試験の実行に耐え得るか否か(プログラムの保守性も含む)を基準に判断し、確認を行う。

—以上—

IV. 入札資料作成要領及び評価手順

「暗号アルゴリズム実装試験ツールの機能追加 (JCATT3の開発)」

入札資料作成要領及び評価手順

目 次

第1章 入札者が提出すべき資料

第2章 提案書の作成要領及び説明

- 2.1 提案書の構成及び記載事項
- 2.2 プロジェクト計画案の作成方法
- 2.3 提案書様式
- 2.4 留意事項

第3章 添付資料の作成要領

- 3.1 個人情報保護体制についての記入方法
- 3.2 情報セキュリティ対策ベンチマーク確認書の記入方法

第4章 評価項目一覧の構成と記載要領

第5章 評価手順

- 5.1 落札方式
- 5.2 総合評価点の配分
- 5.3 技術審査
- 5.4 評価基準
- 5.5 配点構成
- 5.6 合否評価
- 5.7 技術点の算出
- 5.8 総合評価点の算出

第1章 入札者が提出すべき資料

入札者は、独立行政法人情報処理推進機構（以下「機構」という。）が提示する資料を受け、下表に示す資料を作成し、機構へ提示する。

[入札者が機構に提示する資料]

資料名称	資料内容
①委任状 ②入札書	詳しくは入札説明書を参照のこと。
③提案書	仕様書に記述された要求仕様をどのように実現するかを説明したもの。主な項目は以下のとおり。 ・全体方針 ・情報システムの機能等に関する要件の実現方策 ・設計に係る要件の実現方策 ・稼働環境等の要件に対する適合性 別紙：「プロジェクト計画書案」にて作業の体制及び管理方法などについて記載すること。
④添付資料	以下の資料を添付すること。 ・「個人情報保護体制について」 ・「情報セキュリティ対策ベンチマーク確認書」
⑤補足資料（任意提出）	入札者が作成した提案の詳細を説明するための資料。補足資料に記載されている内容は、直接評価されて点数が付与されることはない。 例：担当者略歴、会社としての実績、実施条件等
⑥評価項目一覧	V. 評価項目一覧にて提示している、本件に係る提案をどのような観点・基準で評価するかを取りまとめた表。 評価項目一覧の提出にあたっては、遵守確認欄の記入及び提案書ページ番号欄に該当する提案書のページ番号を記入したものとする。
⑦納税証明書 ⑧登記簿謄本等 ⑨提案書受理票	詳しくは入札説明書を参照のこと。

第2章 提案書の作成要領及び説明

2.1 提案書の構成及び記載事項

次表に、「Ⅴ. 評価項目一覧」から[提案書の目次]の大項目を抜粋したもの及び求められる提案要求事項の概要を示す。提案書は、当該「提案書の目次」に従い、提案要求内容を十分に咀嚼した上で実現可能な内容を記述すること。なお、目次及び要求事項の詳細は、「Ⅴ. 評価項目一覧」を参照すること。

[提案書目次]

提案書 目次項番	大項目	提案要求事項の概要説明
1	全体方針	目標設定、実施作業内容、開発プロセスについて
2	情報システムの機能 等に関する要件の実 現方策	技術的課題のある機能の実現方策
別紙	プロジェクト計画書 案	本件を確実に実施するための、体制、要員、工程計画、工程管理計画、品質保証計画、セキュリティ計画などについて「プロジェクト計画書案」としてまとめたもの。詳細は、2.2プロジェクト計画案の作成方法を参照のこと。 注) この提案書別紙は、採点の対象となる。

2.2 プロジェクト計画案の作成方法

PMBOK等に基づいたプロジェクト計画書案を作成の上、提案書の別紙として提出すること。プロジェクト計画書案は、ひとつの独立したドキュメントとして成立するように構成し、章立てを提案書本文から引き継がずに最初から開始すること。

プロジェクト計画書案には、以下の内容が含まれていることを求める。提案書本文で記述した事項と重複することを妨げない。

また、機構側の体制等、提案時点で知り得ない情報を要するものについては、想定できる範囲内で記述すること。

① 実施体制

- ・作業要員等について、実働可能な人数と役割を含めて図表を用いた記述。
- ・特に再請負により業務の全部または一部を第三者と共同で行う場合には、それぞれの役割分担と関係。
- ・開発の一部を外注する場合、その作業内容。
- ・主要なリーダー/担当者について、担当作業、スキル、略歴
- ・社内外のセキュリティに関する教育の受講歴
- ・コミュニケーション計画及びプロジェクトの意思決定手順

② 工程計画（資源・工数・要員などの計画を含む）

- ・EVMに基づくWBS（ワーク・ブレイクダウン・ストラクチャー。少なくともレベル2、必要に応じてレベル3まで細分化され、かつ作業項目毎に工数、コスト等により定量化されていること）
- ・主要なマイルストーン

③ 工程管理計画

- ・具体的な、WBSディクショナリーの骨子及び進捗評価基準（あるいはその考え方）
ドキュメント一覧（納品物だけでなく、プロジェクト遂行にあたって用いるドキュメントを全て）

④ 品質保証計画

- ・具体的な、ドキュメント作成基準の考え方、ドキュメントレビュー計画、品質評価指標の考え方など

なお、一部のドキュメントについて、発注仕様書において作成基準を指定している場合があるので注意すること。

⑤ セキュリティ計画

- ・実施体制、設計における情報セキュリティ対策の方針前提条件、制約条件及びリスク分析

2.3 提案書様式

- ① 提案書及び評価項目一覧はA4判にて印刷し、特別に大きな図面等が必要な場合には、原則としてA3判にて提案書の中に折り込む。
- ② 提案書については、電子媒体に保存された電子ファイルの提出を求める。その際のファイル形式は、原則として、Microsoft Office形式、Open Office形式またはPDF形式のいずれかとする（これに抛りがたい場合は、機構まで申し出ること）。記録媒体は、CD-RまたはDVD-Rとする。

2.4 留意事項

- ① 機構から連絡が取れるよう、提案書には連絡先（電話番号、FAX番号、及びメールアドレス）を明記する。
- ② 提案書を評価する者が特段の専門的な知識や商品に関する一切の知識を有しなくても評価が可能な提案書を作成する。なお、必要に応じて、用語解説などを添付する。
- ③ 入札者は、提案内容について具体的に提案書本文に記載すること。より具体的・客観的な詳細説明を行うための資料を、提案書本文との対応付けをした上で補足資料として提出することは可能であるが、その際、提案要求事項を満たしているかどうか提案書本文により判断されることに留意すること。例えば、提案書本文に「補足資料〇〇参照」とだけ記載しているものは、提案書に具体的提案内容が記載されていないという評価となる。
- ④ 上記の提案書構成、様式及び留意事項に従った提案書ではないと機構が判断した場合は、提案書の評価を行わないことがある。また、補足資料の提出や補足説明等を求める場合がある。
- ⑤ 提案書、その他の書類は、本入札における総合評価落札方式の技術点評価にだけ使用する。ただし、落札者の提案書（別紙を除く）は契約書に添付する。
- ⑥ 提案書別紙「プロジェクト計画案」については、調整の後に合意形成するものとする。

第3章 添付資料の作成要領

3.1 個人情報保護体制についての記入方法

【様式-A】を用いて作成してください。

「ご回答者連絡先」を記入し、設問に回答（はい、いいえのいずれかを ○ で囲みください。）の上、必要事項の追加記入をお願い致します（※余白を縦横に伸縮してご記入ください）。

なお、本様式は、個人情報の取扱いに関して御社が講じている保護措置について確認することを目的としております。従いまして、設問は応募資格を定めているものではなく、回答の内容により直ちに失格となるということはありません。但し、プロジェクト計画の妥当性評価に用いる場合があります。

3.2 情報セキュリティ対策ベンチマーク確認書の記入方法

本件の担当部署を含む組織体を対象として、情報セキュリティ対策ベンチマーク（<http://www.ipa.go.jp/security/benchmark/index.html>）を実施いただき、その結果をご報告いただきます。【様式-B】に従い作成してください。

なお、本様式は、御社における情報セキュリティに対する取組について確認することを目的としております。従いまして、設問は応募資格を定めているものではなく、回答の内容により直ちに失格となるということはありません。但し、プロジェクト計画の妥当性評価に用いる場合があります。

第4章 評価項目一覧の構成と記載要領

評価項目一覧の構成及び概要説明を以下に記す。「提案書ページ番号」及び「遵守確認欄」については、【入札者が記載する欄】として記載要領をしめしている。

[評価項目一覧の構成と概要]

項目欄名		概要説明
提案書の目次		評価項目一覧の提案書の目次。提案書の構成は、評価項目一覧の構成と同一であること。
評価項目		評価の観点
評価区分	遵守確認事項 (遵守)	本件を実施する上で遵守すべき事項。これら事項に係る内容の提案は求めず、当該項目についてこれを遵守する旨を記述する。
	提案要求事項 (必須)	必ず提案すべき事項。これら事項については、入札者が提出した提案書について、各提案要求項目の評価基準に従い評価し、それに応じた得点配分の定義に従い採点する。 評価ランクDの提案は、不合格とする。
提案書ページ番号		【入札者が記載する欄】 作成した提案書における該当ページ番号を記載する。該当する提案書の頁が存在しない場合には空欄とする。評価者は、本欄に記載されたページを各提案要求事項に係る提案記述の開始ページとして採点を行う。
遵守確認欄		【入札者が記載する欄】 評価区分が「遵守確認事項(遵守)」の場合に、入札者は、遵守確認事項を実現・遵守可能である場合は○を、実現・遵守不可能な場合（実現・遵守の範囲等について限定、確認及び調整等が必要な場合等を含む）には×を記載する。
配点構成及び審査基準		評価区分が「提案要求事項(必須)」の評価項目に対して、どのような基準で採点するかを示している。

第5章 評価手順

5.1 落札方式

次の要件をともに満たしている者のうち、総合評価点の最も高い者を落札者とする。

- ① 入札価格が予定価格の範囲内であること。
- ② 評価項目一覧に記載される評価項目において、「不合格」の項目が無いこと。

5.2 総合評価点の配分

総合評価点	=	技術点	+	価格点
-------	---	-----	---	-----

技術点と価格点の最高点は220点とし、配分は1:1とする。

5.3 技術審査

「V. 評価項目一覧」で示す、評価項目、評価基準、配点構成に基づき、技術審査を行う。

5.4 評価基準

各評価項目には、下表の評価指標に則った評価基準が具体的に設定されている。
この評価基準に基づき、審査員は合議制により各評価項目の評価ランクを決定する。
評価項目によっては、一部の評価ランクを適用しないことが予め決められている場合がある。

評価 ランク	評価指標
S	通常の想定を超える卓越した提案内容であるなど。
A	通常想定される提案として、優位性のある内容である。
B	通常想定される提案としては妥当な提案であると認められる。
C	最低限の記述があると認められる。
D	内容が要件に対して不十分である、明らかに提案要求事項を満たさない、他の提案内容との間に看過できない矛盾がある、遵守確認事項との矛盾がある、あるいは記載がない。(不合格)

5.5 配点構成

評価項目毎に評価ランクに応じた得点が決定される。

各評価項目における配点構成は、「評価項目一覧」の「配点構成」欄にて定義されている。

5.6 合否評価

評価ランクDが設定されている評価項目について、評価ランクがDとなった場合には、不合格となる。入札者は、提案書にて要件を全て充足することを示さなければならない。一つでも要件が充足できないとみなされた場合は、その提案は不合格となる。

5.7 技術点の算出

ランクD（不合格）の評価が無い提案について、全ての評価項目における得点を合計し、これを技術点とする。

5.8 総合評価点の算出

以下を合計し、総合評価点を算出する。

- ① 「5.7 技術点の算出」により与えられる技術点（配点：220点）
- ② $220\text{点} \times (1 - \text{入札価格} \div \text{予定価格})$ により得た数値の小数点以下2位を切り捨てて算出した価格点

【様式-A】

個人情報保護体制について

本様式は、個人情報の取扱いに関して御社が講じている保護措置について確認することを目的としております。お手数ですが、最初に「ご回答者連絡先」を記入し、以下の設問に回答（はい、いいえのいずれかを○で囲みください。）の上、必要事項の追加記入をお願い致します。

余白を縦横に伸縮してご記入ください。

ご回答者連絡先

組 織 名	
部 署 名	
氏 名	
連絡先電話番号	
メールアドレス	

Q 1. 個人情報保護に係るプライバシーポリシー・規程・マニュアルはございますか。

【 は い ・ いいえ 】

「は い」を○で囲んだ方は、以下の事項を記入してください。

以下に名称、作成年月日、作成の参考にした業界ガイドライン（名称・作成機関名）を記入してください。

【個人情報保護に関するプライバシーポリシー・規程・マニュアル】

Q 2. 個人情報保護に係る組織内体制はありますか。

【 は い ・ いいえ 】

「は い」を○で囲んだ方は、以下の事項を記入してください。

以下に担当部門、役職名、役割、担当業務範囲を記入してください。

【個人情報保護に係る組織内体制】

Q 3. 個人情報を取扱う従事者（派遣職員、アルバイトを含む）への教育・研修を実施しておりますか。

【 は い ・ いいえ 】

「は い」を○で囲んだ方は、以下の事項を記入してください。

以下に実施部門、開催時期・年間回数、対象者、使用テキストを記入してください。

【個人情報保護に係る従事者への教育・研修体制】

Q 4. 個人情報保護に係る監査規程はありますか。

【 は い ・ いいえ 】

「は い」を○で囲んだ方は、以下の事項を記入してください。

以下に監査規程（名称、制定年月日）を記入してください。また、すでに監査の実績がある場合は、直近の監査実施日を記入してください。

【個人情報保護に係る監査規程・直近の監査実施日】

Q 5. 情報処理システムの安全対策はありますか。

【 は い ・ いいえ 】

「は い」を○で囲んだ方は、以下の事項を記入してください。

【情報処理システムの安全対策】

「いいえ」と回答した設問に対して、このたびの IPA からの個人情報を取扱う業務を実施する上でご検討されている保護措置の案があれば以下にご記入ください。形式は自由です。余白を縦横に伸縮してご記入ください。

【今回の個人情報を取扱う業務でご検討されている保護措置案】

Q 6. 認定団体からプライバシーマークを付与されておりますか。

【 は い ・ いいえ 】

「は い」を○で囲んだ方は、以下の事項を記入（上書き）してください。

認定番号：○○○○○○○○

有効期間：○○○○年○○月○○日 ～ ○○○○年○○月○○日

【様式－B】

平成 年 月 日

[会社名]

[責任者役職・氏名]

情報セキュリティ対策ベンチマーク確認書

情報セキュリティ対策ベンチマークを実施し、下記の評価結果に相違ないことを確認します。

記

1. 確認日時

平成 年 月 日 【実際に確認を行った日時】

2. 確認対象

【情報セキュリティ対策ベンチマークの確認を行った範囲について記載
(例、本件業務を請け負われる部署を含む組織体等の名称)】

3. 情報セキュリティ対策ベンチマーク実施責任者

【情報セキュリティ対策ベンチマークによる確認を実施した者。】

4. 確認結果

全項目に係る平均値：

なお、ベンチマーク実施出力結果を別紙として添付します。

V. 評価項目一覧

提案書の目次			評価項目	評価区分	提案書 ページ番号	遵守 確認欄	配点構成および評価基準				
大 項 目	中 項 目	小 項 目					S	A	B	C	D
1. 全体方針											
	1.1	開発プロセス									
	1.1.1	開発業務の範囲について、「開発業務内容」に記載している項目を一括して受託すること(部分についての提案は認めない)	遵守			合格 遵守確認欄が「○」の場合				不合格 遵守確認欄が「×」の場合	
	1.1.2	全体プロセスの特徴、本件に採用した理由は明確かつ適切であるか。	必須			10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。 本件の状況を考慮して、開発プロセスに独自のカスタマイズがかけられているなど、本件に適用する理由と効果が明確になっている。	4 全体プロセスの特徴が記載されている。 社内規準あるいは業界規準に準拠している。	0 左記Bの基準を満たしていない。	不合格	
	1.1.3	開発手法やテスト方法は具体的かつ実行可能であるか。 採用するプロジェクト管理ツールや開発支援ツールは適切であるか。	必須			10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。 選択された開発手法・テスト方法に合わせてプロジェクト管理ツールや開発支援ツールが仮定され、その選択理由や効果、選択したツールの導入実績についても説明されている。	4 本件の特徴を考慮して、採用する開発手法・テスト方法が選択されており、具体的かつ実行可能な内容となっている。	0 左記Bの基準を満たしていない。	不合格	
2. 情報システムの機能等に関する要件の実現方策											
	2.1	機能要件									
	2.1.1	Ⅲ 仕様書 に記載された機能要件を全て実現すること。	遵守			合格 遵守確認欄が「○」の場合				不合格 遵守確認欄が「×」の場合	
3. 作業の体制及び管理(プロジェクト計画案)											
	3.1	実施体制									
	3.1.1	体制図は十分に詳細化され、開発、工程管理、品質保証、セキュリティ対策等の活動を適切に実施できるよう、役割・責任が明記されているか。 プロジェクトメンバーは、本件実施に十分な経験を持つことが説明されているか。	必須			10 右記Aの基準を満たしている。 詳細設計開始時点の構成要員は決定し、組織体制図に氏名あるいはそれに準ずる情報を明記している。	7 右記Bの基準を満たしている。 設計・開発、工程管理、品質保証、セキュリティ対策等の活動について役割分担がなされている。 プロジェクトメンバーは、上記の役割分担に応じた実務経験を有する。	4 提案する体制図において、各グループ及び構成要員の役割、責任を明確にしている。 プロジェクトメンバーの実務経験が記載されている。	0 左記Bの基準を満たしていない。	不合格	
	3.1.2	プロジェクトメンバーの中に暗号技術に知見がある要員が含まれているか。(ヒアリングと合わせて評価を実施する予定)	必須			10 右記Aの基準を満たし、かつ、その経験が充実している。	7 右記Bの基準を満たしている。 暗号技術の適用/応用に係る実務を経験している。	4 暗号技術に知見がある要員が含まれている。	0 左記Bの基準を満たしていない。	不合格	
	3.1.3	コミュニケーション計画及びプロジェクトの意思決定手順が示されているか。	必須			10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。 対象者の具体的な役割などに基づいて記載されている。	4 適切なコミュニケーション計画及びプロジェクトの意思決定手順が記載されている。	0 左記Bの基準を満たしていない。	不合格	
	3.2	プロジェクトマネージャのスキル(ヒアリングと合わせて評価を実施する予定)									

3.2.1	システム開発経験:プロジェクトマネージャーは、本件システムと同等規模(利用ユーザー数、トランザクション数、要求される信頼性等)のシステムの開発・運用をどれくらい実施した経験があるか。 プロジェクト経験については、成功したプロジェクトのみが記述されているか。また、その際、プロジェクトの成功を証明する資料を添付されているか。	必須			10 右記Aの基準を満たし、かつ、その能力が卓越している。	7 右記Bの基準を満たしている。 プレゼンテーションを通じて、自分のシステム開発に関する能力(知識・スキル・経験)を本プロジェクトで発揮できることを示している。	4 プロジェクトマネージャーは本件システムと同等規模のシステム開発プロジェクトの経験を5年以上有している。 プロジェクトマネージャーは、それらのプロジェクトの成功に貢献したポイントを提示している。	0 左記Bの基準を満たしていない。	不合格
3.2.2	プロジェクトマネージャーは、PMBOK・EVMに基づいたプロジェクト管理の経験をどれくらい有しているか。 プロジェクト経験については、成功したプロジェクトのみが記述されているか。また、その際、プロジェクトの成功を証明する資料を添付されているか。	必須			10 右記Aの基準を満たし、かつ、その能力が卓越している。	7 右記Bの基準を満たしている。 プレゼンテーション/質疑応答を通じて、自分のPMBOK・EVMに関する能力(知識・スキル・経験)を発揮している。 プレゼンテーション/質疑応答を通じて、自分のプレゼンテーション力・質問対応力・課題に対する対応策を立案していく能力等を発揮している。	4 プロジェクトマネージャーはPMBOK・EVMに基づいたプロジェクト管理の経験を一通り(計画、実行、評価、改善)有していることが示されている。 プロジェクトマネージャーは、それらのプロジェクトマネジメントを成功させたことを提示している。	0 左記Bの基準を満たしていない。	不合格
3.2.3	プロジェクトマネージャーは、本プロジェクトのポイントを明確に説明できるか。その内容は適切か。 プロジェクトマネージャーは、本プロジェクトにおける成功要因及びリスクを把握できているか。	必須			10 右記Aの基準を満たし、かつ、その能力が卓越している。	7 右記Bの基準を満たしている。 プレゼンテーション/質疑応答を通じて、自分のプロジェクトの深い理解度を発揮している。	4 提案書の中で、本プロジェクトのポイント・成功要因・リスクを端的に説明している。	0 左記Bの基準を満たしていない。	不合格
3.3 工程計画(資源・工数・要員などの計画を含む)									
3.3.1	WBS単位にスケジュールが作成されているか。 作業項目の順序や依存関係は明確かつ適切に設定されているか。	必須			10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。 各WBSの作業順序や依存関係が整理され、手戻りがないように工夫を行っている。	4 WBSのタスク単位で、成果物作成に必要な工数を適切に見積もり、妥当なスケジュールを作成している。	0 左記Bの基準を満たしていない。	不合格
3.3.2	WBS構造は発注者から提示された「WBSレベル」にしたがって設定されているか。 WBSは適切な単位のWPIに分割されているか。	必須			10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。 WBSは適切な単位のWPIに分割されており、かつ、詳細化が必要な部分については、適切なレベルで詳細化を行っている。	4 発注者から提示された「WBSレベル」にしたがってWBSが作成されている。	0 左記Bの基準を満たしていない。	不合格
3.3.3	WBS単位でコスト(または工数)が明記されているか。 コスト全体に対する各WBSの配分は適切であり、また、リスクに応じたリザーブを適切に見込んでいるか。	必須			10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。 算出されたコストは、作業工数×人月単価によって、正確に見積もっている。	4 WBS単位でコスト(または工数)が明記され、配分は適切である。	0 左記Bの基準を満たしていない。	不合格
3.4 工程管理計画(WBSディクショナリ)									
3.4.1	計測規準(進捗評価基準)の考え方が示されているか。その内容は適切か。	必須			10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。 作成終了をもって完了とせず、レビューや検証、検査に要する工程を見込んでいる。	4 成果物の種類ごとに、計測基準が定められている。	0 左記Bの基準を満たしていない。	不合格
3.4.2	WBS単位の成果物は明確かつ適切に設定されているか。 成果物の記載内容が定義され、サンプル成果物などが具体的に示されているか。	必須			10 右記Aの基準を満たし、かつ、一般的な中間成果物等について、サンプルが提示されている。	7 右記Bの基準を満たしている。 WBS単位の成果物に、納入物件以外の中間成果物等が適切に設定されている。	4 WBS単位の成果物は、少なくとも納入物件について明確に設定されている。	0 左記Bの基準を満たしていない。	不合格
3.5 ドキュメント一覧									
3.5.1	納入物以外のドキュメント、管理台帳、連絡票などについて、網羅的に記述されているか。	必須			10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。 定義されたドキュメントの利用目的が端的に記載されている。	4 会議体に提出する資料、課題整理に用いる台帳、連絡書式など、プロジェクト遂行に必要なドキュメントが定義されている。	0 左記Bの基準を満たしていない。	不合格
3.6 品質保証計画									

3.6.1	品質管理に必要と思われる体制、活動内容は具体的かつ実現可能であるか。	必須		10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。提案する品質管理業務の活動を行った結果としての実効性について説明されている。	4 品質管理業務を適切に実施する為に必要となる品質管理体制、活動内容が具体的に記載され、かつ、実現可能であることが説明されている。	0 左記Bの基準を満たしていない。	不合格
3.6.2	ドキュメント作成基準について、様式、書き方などの考え方が示されているか。当該基準は全社的(あるいはそれに匹敵する規模の組織、例えば事業所、事業部などにおける)基準に基づくなど、統一的なものか。	必須		10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。社内規準などに基づく、雛形、作成基準が具体的に示されている。	4 ドキュメントの作成基準についての考え方が記載され、本プロジェクトのみに有効ではないことが示されている。	0 左記Bの基準を満たしていない。	不合格
3.6.3	ドキュメントレビュー計画について、適切に詳細化されているか。作成担当部門による自己評価のみで終わってしまうことはないか。	必須		10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。社内規準などに基づいて、担当部署・グループ内でのレビューだけでなく、品質管理部門あるいは社外コンサルタントのレビューを受けることとなっているか。基準には、レビュー結果の様式、機能分割の適切性の観点が含まれている。	4 ドキュメントのレビュー計画について、体制、コミュニケーション計画に記載されている内容が詳細化され、レビュー手順の考え方が記載されている。	0 左記Bの基準を満たしていない。	不合格
3.6.4	ソースコードレビュー計画について、適切に詳細化されているか。作成担当部門による自己評価のみで終わってしまうことはないか。	必須		10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。次の項目がレビュー観点に含まれている。 1)ソースコードの可読性(複雑度)を適切と判断する定量的な基準 2)エラー処理が適切に行われているか 3)メモリリークが発生しないか	4 ソースコードのレビュー計画について、レビュー体制(レビュー者のスキルを含む)、レビュースケジュール及び頻度、レビュー観点が明確になっている。	0 左記Bの基準を満たしていない。	不合格
3.6.5	品質評価のための指標・基準が提示されているか。その内容は適切か。	必須		10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。社内規準などに基づいた具体的な提示され、基準、目標値等が設定されている。	4 品質評価指標についての考え方が記載されている。	0 左記Bの基準を満たしていない。	不合格
3.6.6	テスト方針、検証方法・指標、目標値に関して効果的かつ効率的な提案がなされている。目指すべき機能、性能等に対して、正しい目標値が設定されている。	必須		10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。提案内容は、効果的かつ効率的である。	4 テスト方針、検証方法・指標、目標値に関して具体的な提案がなされている。目指すべき機能、性能等に対して、正しい目標値が設定されている。	0 左記Bの基準を満たしていない。	不合格
3.7 セキュリティ計画								
3.7.1	実施体制における情報セキュリティ対策として、関連ドキュメントのアクセス管理、コーディング規約の制定などがなされているとともに、それらの効率的運用のための方策が計画されているか。	必須		10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。それらの効率的運用のための方策が計画されている。	4 関連ドキュメントのアクセス管理、コーディング規約の制定などがなされている。	0 左記Bの基準を満たしていない。	不合格
3.7.2	ソフトウェアの設計にあたり、その情報セキュリティに関する妥当性を確認するための設計レビューの範囲及び方法について、具体的に提案されているか。	必須		10 右記Aの基準を満たし、かつ、提案内容が卓越している。	7 右記Bの基準を満たしている。他のレビューから独立した計画となっており、それらの効率的運用のための方策が計画されている。	4 情報セキュリティに関連する機能・性能等に関するレビューの計画について、その範囲及び方法が具体的に記載されている。	0 左記Bの基準を満たしていない。	不合格

配点構成

評価基準に照らして評価し、加点する。(満点：220点)

評価:S評価:10点、A評価:7点、B評価:4点、C評価:0点、D評価:不合格

VI. その他関係資料

独立行政法人 情報処理推進機構
入札心得
(総合評価落札方式)

(趣 旨)

第1条 当機構の契約に係る一般競争又は指名競争（以下「競争」という。）を行う場合において、入札者が熟知し、かつ遵守しなければならない事項は、法令に定めるもののほか、この心得に定めるものとする。

(仕様書等)

第2条 入札者は、仕様書、図面、契約書案及び添付書類を熟読のうえ入札しなければならない。

2 入札者は、前項の書類について疑義があるときは、関係職員に説明を求めることができる。

3 入札者は、入札後、第1項の書類についての不明を理由として異議を申し立てることができない。

(入札保証金及び契約保証金)

第3条 入札保証金及び契約保証金は、全額免除する。

(入札の方法)

第4条 入札者は、別紙様式による入札書を直接又は郵便等で提出しなければならない。

(入札書の記載)

第5条 落札決定に当たっては、入札書に記載された金額に当該金額の5パーセントに相当する額を加算した金額をもって落札価格とするので、入札者は消費税に係る課税事業者であるか免税事業者であるかを問わず、見積もった契約金額の105分の100に相当する金額を入札書に記載すること。

(直接入札)

第6条 直接入札を行う場合は、入札書を封筒に入れ、封緘のうえ入札者の氏名を表記し、予め指定された時刻までに契約担当職員等に提出しなければならない。

この場合において、入札書とは別に提案書及び証書等の書類を添付する必要がある入札にあつては、入札書と併せてこれら書類を提出するものとする。

2 入札者は、代理人をして入札させるときは、その委任状を持参させなければならない。

(郵便等入札)

第7条 郵便等入札を行う場合には、二重封筒とし、入札書の中封筒に入れ、封緘のうえ入札者の氏名、宛先、及び入札件名を表記し、予め指定された時刻までに到着するように契約担当職員等あて書留で提出しなければならない。この場合において、入札書とは別に提案書及び証書等の書類を添付する必要がある入札にあつては、入札書と併せてこれら書類を提出するものとする。

2 入札者は、代理人をして入札させるときは、その委任状を同封しなければならない。

(代理人の制限)

第8条 入札者又はその代理人は、当該入札に対する他の代理をすることができない。

2 入札者は、予算決算及び会計令（昭和22年勅令第165号、以下「予決令」という。）第71条第1項各号の一に該当すると認められる者で、その事実があった後2年を経過しない者を入札代理人とすることができない。

(条件付きの入札)

第9条 予決令第72条第1項に規定する一般競争に係る資格審査の申請を行ったものは、競争に参加する者に必要な資格を有すると認められること又は指名競争の場合にあつては指名されることを条件に入札書を提出することができる。この場合において、当該資格審査申請書の審査が開札日までに終了しないとき又は資格を有すると認められなかったとき若しくは指名されなかったときは、当

該入札書は落札の対象としない。

(入札のとりやめ等)

第10条 入札参加者が連合又は不穩の行動をなす場合において、入札を公正に執行することができないと認められるときは、当該入札者を入札に参加させず又は入札の執行を延期し、若しくはとりやめることがある。

(入札の無効)

第11条 次の各号の一に該当する入札は、無効とする。

- (1) 競争に参加する資格を有しない者による入札
- (2) 指名競争入札において、指名通知を受けていない者による入札
- (3) 委任状を持参しない代理人による入札
- (4) 記名押印（外国人又は外国法人にあっては、本人又は代表者の署名をもって代えることができる。）を欠く入札
- (5) 金額を訂正した入札
- (6) 誤字、脱字等により意思表示が不明瞭である入札
- (7) 明らかに連合によると認められる入札
- (8) 同一事項の入札について他人の代理人を兼ね又は2者以上の代理をした者の入札
- (9) 入札者に求められる義務を満たすことを証明する必要がある入札にあっては、証明書が契約担当官等の審査の結果採用されなかった入札
- (10) 入札書受領期限までに到着しない入札
- (11) その他入札に関する条件に違反した入札

(開 札)

第12条 開札には、入札者又は代理人を立ち合わせて行うものとする。ただし、入札者又は代理人が立会わない場合は、入札執行事務に関係のない職員を立会わせて行うものとする。

(調査基準価格、低入札価格調査制度)

第13条 工事その他の請負契約（予定価格が1千万円を超えるものに限る。）について予決令第85条に規定する相手方となるべき者の申込みに係る価格によっては、その者により当該契約の内容に適合した履行がされないこととなるおそれがあると認められる場合の基準は次の各号に定める契約の種類ごとに当該各号に定める額（以下「調査基準価格」という。）に満たない場合とする。

- (1) 工事の請負契約 その者の申込みに係る価格が契約ごとに3分の2から10分の8.5の範囲で契約担当官等の定める割合を予定価格に乗じて得た額
- (2) 前号以外の請負契約 その者の申込みに係る価格が10分の6を予定価格に乗じて得た額
- 2 調査基準価格に満たない価格をもって入札（以下「低入札」という。）した者は、事後の資料提出及び契約担当職員等が指定した日時及び場所で実施するヒアリング等（以下「低入札価格調査」という。）に協力しなければならない。
- 3 低入札価格調査は、入札理由、入札価格の積算内訳、手持工事の状況、履行体制、国及び地方公共団体等における契約の履行状況等について実施する。

(落札者の決定)

第14条 契約担当職員等が採用できると判断した提案書を入札書に添付して提出した入札者であつて、その入札金額が予決令第79条の規定に基づいて作成された予定価格の制限の範囲内で、かつ提出した提案書と入札金額を当該入札説明書に添付の評価手順書に記載された方法で評価、計算し得た評価値が最も高かった者を落札者とする。

- 2 低入札となった場合は、一旦落札決定を保留し、低入札価格調査を実施の上、落札者を決定する。
- 3 前項の規定による調査の結果その者により当該契約の内容に適合した履行がされないおそれがあると認められるとき、又はその者と契約を締結することが公正な取引の秩序を乱すこととなるおそれがあつて著しく不適當であると認められるときは、予定価格の制限の範囲内の価格をもって入札をした他の者のうち、評価の最も高い者を落札者としてすることがある。

(再度入札)

第15条 開札をした場合において、各人の入札のうち予定価格の制限に達した価格の入札がないとき

は、直ちに再度の入札を行う。なお、開札の際に、入札者又はその代理人が立ち会わなかった場合は、再度入札を辞退したものとみなす。

2 入札者は、代理人をして再度入札させるときは、その委任状を持参させなければならない。

(同総合評価点の入札者が2者以上ある場合の落札者の決定)

第16条 落札となるべき同総合評価点の入札をした者が2者以上あるときは、直ちに当該入札をした者又は第12条ただし書きにおいて立ち会いをした者にくじを引かせて落札者を決定する。

2 前項の場合において、当該入札をした者のうちくじを引かない者があるときは、これに代わって入札事務に関係のない職員にくじを引かせるものとする。

(契約書の提出)

第17条 落札者は、契約担当職員等から交付された契約書に記名押印（外国人又は外国法人が落札者である場合には、本人又は代表者が署名することをもって代えることができる。）し、落札決定の日から5日以内（期終了の日が行政機関の休日に関する法律（昭和63年法律第91号）第1条に規定する日に当たるときはこれを算入しない。）に契約担当職員等に提出しなければならない。ただし、契約担当職員等が必要と認めた場合は、この期間を延長することができる。

2 落札者が前項に規定する期間内に契約書を提出しないときは、落札は、その効力を失う。

(入札書等に使用する言語及び通貨)

第18条 入札書及びそれに添付する仕様書等に使用する言語は、日本語とし、通貨は日本国通貨に限る。

(落札決定の取消し)

第19条 落札決定後であっても、この入札に関して連合その他の事由により正当な入札でないことが判明したときは、落札決定を取消すことができる。

以上

(参 考)

予算決算及び会計令【抜粋】

(一般競争に参加させることができない者)

第70条 契約担当官等は、売買、貸借、請負その他の契約につき会計法第二十九条の三第一項の競争（以下「一般競争」という。）に付するときは、特別の理由がある場合を除くほか、当該契約を締結する能力を有しない者及び破産者で復権を得ない者を参加させることができない。

(一般競争に参加させないことができる者)

第71条 契約担当官等は、一般競争に参加しようとする者が次の各号のいずれかに該当すると認められるときは、その者について三年以内の期間を定めて一般競争に参加させないことができる。その者を代理人、支配人その他の使用人として使用する者についても、また同様とする。

一 契約の履行に当たり故意に工事若しくは製造を粗雑にし、又は物件の品質若しくは数量に関して不正の行為をしたとき。

二 公正な競争の執行を妨げたとき又は公正な価格を害し若しくは不正の利益を得るために連合したとき。

三 落札者が契約を結ぶこと又は契約者が契約を履行することを妨げたとき。

四 監督又は検査の実施に当たり職員の職務の執行を妨げたとき。

五 正当な理由がなくて契約を履行しなかつたとき。

六 この項（この号を除く。）の規定により一般競争に参加できないこととされている者を契約の締結又は契約の履行に当たり、代理人、支配人その他の使用人として使用したとき。

2 契約担当官等は、前項の規定に該当する者を入札代理人として使用する者を一般競争に参加させないことができる。